Guidance on Nonfederal Privacy Impact Assessment (PIA)

Version 1.1 (800-171): August 6, 2020

Instructions for GSA Vendors:

GSA requires vendors to conduct privacy impact assessments (PIAs) for electronic information systems and collections in accordance withCIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. Vendors may use this or their own templates/forms to meet the requirement. However, 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 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 reserves the right to publish and/or link to the final product on its public website www.gsa.gov/PIA.

This guidance is provided for the benefit of vendors maintaining nonfederal systems and offers an opportunity for vendors to highlight the data protection, privacy by design, data minimization and similar principles that their services may employ. The PIA is a necessary step in becoming a GSA service provider, in accordance with the Blanket Purchase Agreement (BPA).

This guidance is designed for nonfederal systems described in National Institutes of Standards and Technology (NIST) Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". PIAs are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form.

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):

Name of GSA Program Manager:

GSA Chief Privacy Officer (CPO):

800-171 PIA Template Document Revision History

Date	Description	Version of Template
06/10/2020	Initial Draft of Non-Federal System PIA	1.0

Table of contents

Version 1.1 (800-171): August 6, 2020

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 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.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

SECTION 8.0 AWARENESS AND TRAINING

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

SECTION 9.0 ACCOUNTABILITY AND AUDITING

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

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.

A. System, Application, or Project Name: Lyft Rideshare

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

Federal employees who are users of the Lyft platform.

C. 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;
- 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.

Other Information (health, medical information).

Other types of Controlled Unclassified Information as listed in the CUI Registry, such as:

Physical Security and protection of federal buildings
Emergency Management and Continuity of Operations
Information Systems Vulnerability Government
Financial/Fiscal Information International Agreements
Legal Procurement/Acquisition Proprietary Business Information]

Overview

[The overview is a short description of the system, application, or project. At a minimum, the overview must include:

- *Descriptions of its purpose(s) – why this system, application, technology, pilot, program, or other collection (project) is being completed; what legislation authorizes it; and how it relates to the GSA's mission of providing the best value for government and the American people;*

Lyft provides on-demand ridesharing and ride-hailing services by matching drivers and riders via a mobile application.

- *Descriptions of what PII is collected, its maintenance, use, or its dissemination and who or what it is collected from; and,*

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). communications

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

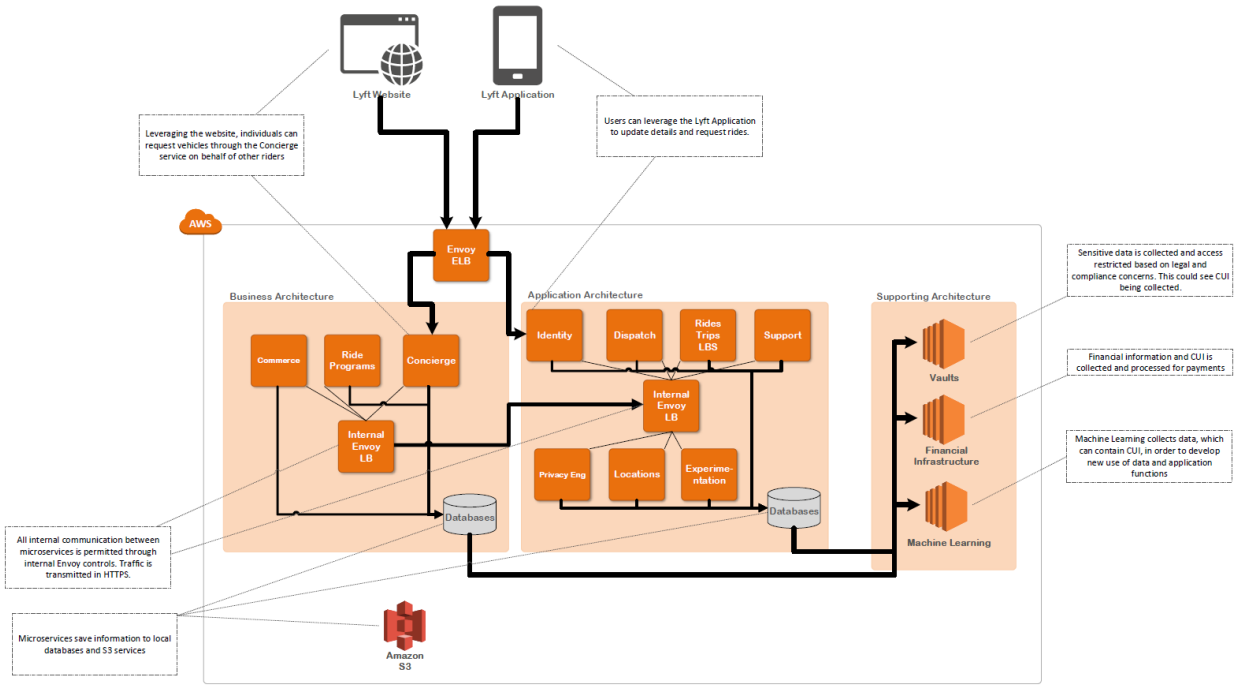
- Location information (device's precise location when the app is open and in use, including while the app is running in the background from the time the user requests a ride until it ends)
- Usage information (including ride information like the date, time, destination, distance, route, payment, and 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, including the participants' phone numbers, the date and time, and the contents of 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, 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 third parties:

- 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 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.

● *Descriptions of how the system, application, or project collects and uses PII, including an example that illustrates what happens to the PII from the time it is collected until it is destroyed.]*



Lyft will receive a secure transmission from each federal customer with the email addresses of employees in the agency's expense management system. If this email is already associated with a Lyft account, no action is taken - however, if this is a new email, then Lyft sends an invitation to create a business profile. 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. The process to match a rider with a driver begins with the rider providing their location information, either by turning on their phone's location services or manually entering their pickup location. They must then provide their destination (either by manual entry or choosing a location from a list of suggested options). The rider may then select the ride type (e.g. shared ride) and then confirm their ride request. The rider will be able to see in the app which profile they're currently in and which payment method that will be applied. The Lyft platform matches the rider with a driver based on the user's selection as well as the driver's location. Once the ride is completed, the rider's app will surface a payment screen which displays the payment method, the ride price, and allows the user to add a tip and provide feedback about the ride in the form of a star rating and free text. The payment screen will also allow the user to select either the business or personal profile (or switch from one to the other). Once the user taps the submit button, Lyft receives the payment and rating information and emails the user a receipt.

Lyft uses personal information in order to:

- Provide the Lyft platform, which includes:
    - Verifying user identity and maintaining user accounts, settings, and preferences;
    - Connecting users to rides and tracking their progress;
    - Calculating prices and processing payments;
    - Allowing riders and drivers to connect regarding their ride and to choose to share their location with others;
    - Communicate with users and collect feedback about their rides and experiences,
    - Facilitate additional services and programs with third parties and operate

contests, sweepstakes and other promotions.

- Maintain the security and safety of the platform and its users, which includes:
    - Authenticating users;
    - Verifying that drivers and their vehicles meet safety requirements,
    - Investigate and resolve incidents, accidents, and insurance claims,
    - Encourage safe behavior;
    - Finding and preventing fraud;
    - Blocking and removing unsafe or fraudulent users.
- Maintaining the Lyft community, which includes
    - Communicating about events, promotions, elections and campaigns;
    - Personalize and provide content, experiences, communications and advertising to promote and grow the Lyft platform;
    - Help facilitate donations users choose to make through the Lyft platform.
- Providing customer support, which includes:
    - Investigating and assisting in resolving questions or issues;
    - Providing user support;
- Improving the Lyft platform, which includes:
    - Performing research, testing and analysis,
    - Developing new products, features, partnerships and services,
    - Preventing, finding and resolving software or hardware bugs and issues, and
    - Monitoring to improve operations and processes, including security practices, algorithms and other modeling.
- Responding to legal proceedings and requirements when the law, government entities, or other regulatory bodies impose demands and obligations on Lyft with respect to its services.

SECTION 1.0 PURPOSE OF COLLECTION

1.1 What legal authority and/or contractual agreements allow GSA to offer the vendor's services?

Pursuant to Federal Acquisition Regulation FAR 13.303 GSA is authorized to award Blanket Purchase Agreements to Uber Technologies, Inc (Supplier) and Lyft Inc (supplier), abiding by the terms and conditions of the multiple awards BPA.

1.2 Explain how long and for what reason the information is retained.

The Government will maintain records in accordance with the National Archives and Records Administration policy. The Rideshare/Ride-hail BPA Holder(s) must maintain records in accordance with FAR Subpart 4.7 Contractor Records Retention and make available for examination pursuant to FAR 52.212-5(d).

SECTION 2.0 OPENNESS AND TRANSPARENCY

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

Potential riders will receive an invite 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.

If the information is collected from someone other than the individual explain how that information is collected, maintained, used, or disseminated (e.g., via application programming interface/API) and how the individual was notified of the use of the information being collected.]

The federal agency managing the travel program will provide Lyft with email addresses of eligible employees via SFTP.

Lyft's Privacy Policy provides comprehensive notice of how and when it exchanges information with third parties. Users must accept the Lyft Terms of Service and Privacy Policy prior to creating an account and taking any rides on the platform.

SECTION 3.0 DATA MINIMIZATION

3.1 Why is the collection and use of the 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 (in order 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 picture 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.

3.2 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. Detailed information about rider location is available on the Lyft website: https://help.lyft.com/hc/en-us/articles/360046897454-Rideshare-Passenger-Location.

3.3 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 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.

3.4 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 3.3., 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 to 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 4.0 LIMITS ON USING AND SHARING INFORMATION

4.1 Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?

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.

4.2 Will the vendor share any of the information with other individuals, federal and/or state agencies, or private-sector organizations? If so, how will the vendor share the information?

Lyft will provide customer agencies with transaction reports with ride details, 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.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is 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;
- In order 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 5.0 DATA QUALITY AND INTEGRITY

5.1 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 6.0 SECURITY

Customer agencies that would like to review security documents can request access from the Program Management Office through the rideshare.ridehail@gsa.govemail box.

Dedicated reading room sessions can be provided to interested customer agencies in order to view current security documents.

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 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.

7.2 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).

7.3 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 8.0 AWARENESS AND TRAINING

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

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

SECTION 9.0 ACCOUNTABILITY AND AUDITING

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

Lyft has the following protections in place to safeguard information:

1. Role-based access controls that 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 (HIPAA and SOC 2 Type II).

[1]OMB Memorandum *Preparing for and Responding to the Breach of Personally Identifiable Information*(OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad." [2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.