Privacy initiative and procurement form (Beta v0.2)

Fill out the form below when seeking approval for an initiative or procurement solution (referred to generally as “solutions”) that involves the collection, storage, processing, analysis, sharing, or other use of data or information (referred to generally as “usage of data”).

If any questions while filling out form, contact the Digital Privacy Officer. Once completed, email this form to the Digital Privacy Officer at digitalprivacy@sanjoseca.gov.

Section 1

Main point of contact for solution

Name (first and last): [redacted]

Department: San Jose Police Department

Title: Division Manager

Email: [redacted]

Phone: [redacted]

Summarize the purpose of the data solution below:

For example, is this data solution meant to inform traffic decisions, share previously private data to the public, monitor a program’s progress, track student success, evaluate the equity of a program’s impact?

The Vigilant License Plate Reader (LPR) commercial database will be used to augment the investigation of crime, identifying where and when license plates have been identified in the commercial database. San Jose will not be contributing any data to the commercial database, only accessing the database.

Where is the data used originating? Mark all that apply

☐ Public data sources (e.g., US Census, CDC, any data readily accessible online) – **list all public data sources used below**. For data accessed on the internet, provide a URL through which the data can be accessed. Do not provide a direct download link, but to the page that provides a download/export link.

☐ Private data (not public) collected exclusively on City employees or programs (e.g., outcome metrics of a department or program); this includes publishing data for public viewing – fill out Section 2

☒ Private data shared **from** a non-City entity (e.g., vendor) – fill out Sections 2 and 3

☐ Private data shared **to** another non-City entity – fill out Sections 2 and 3

☐ Collecting new data on non-City employees (either directly, via another department, or through a non-City entity) – fill out Sections 2 and 4

Section 2

If any data used is Private (i.e., not readily accessible to the public at this time), answer the following:

Will the solution involve the sharing of Personally Identifiable Information (PII) to or from a party (e.g,. vendor, public)? PII includes any information that can directly or indirectly identify an individual, such as one's name or address. Refer to the table on the following page for types of PII.

☒ Yes (mark the relevant PII categories and sub-categories below)

☐ No

Is there an underlying dataset which includes PII that is directly linked to the data shared?

☐ Yes (mark the relevant PII categories and sub-categories below)

☒ No

☐ Uncertain (contact the Digital Privacy Officer to discuss)

If answered "Yes" to either question above, fill out the table on the following page

Detail which of the following Personally Identifiable Information (PII) this solution uses:

Category of PII	Sub-categories
□ Personal Data	□ Full name; □ Home address; □ Email address; □ Phone, laptop, or other device IP[1] address; □ Government-Issued ID # (e.g., Driver's License, Passport, Social Security Number); □ Employee ID number; 🟥 License Plate □ Credit or debit card information; □ Bank account, brokerage account or other financial information; □ Date of birth; □ Place of birth; □ Other written or scanned information that can directly tie to an individual or household
□ Sensitive PII or demographic-related PII – **NOTE:** Ignore if data is only shared in aggregate of a population larger than 1,000[2] (e.g., # of registered voters in San José)	□ Biometric data; □ Genetic data; □ Physical identifiable characteristics; □ Other health records □ Race or ethnic origin; □ Nationality; □ Immigration status; □ Religious affiliation; □ Political affiliation; □ Voter status; □ Education records □ Criminal records □ Other sensitive written or scanned information traditionally kept confidential
□ Image data	🟥 Picture that can identify an individual by their face or other physical and contextual information[3]
□ Recording data	□ Video that can identify an individual by their face or other physical and contextual information; □ Audio that can identify an individual by their voice or other contextual information
□ Geolocation data	🟥 Data affiliated with a vehicle, computer, or other device that can be used to identify an individual's physical location
🟥 Other private or personal information	*Detail other data that could directly or indirectly identify an individual:* Vehicle make, model, color and/or distinguishing/unique characteristics.

[1] Internet Protocol - An IP address is a unique address that identifies a device on the internet or a local network

[2] Based on reporting requirements used for anonymity by the US Department of Health and Human Services AFCARS Foster Care Dataset; refer to the 2021 codebook, element #6

[3] An example of "contextual information" being used to identify someone could include a picture of a license plate, or a picture of someone's backside next to a house with a visible address.

Section 3

If using private data shared from or to another department or non-City entity, answer the following:

Does this solution involve the sharing of any PII as defined in Section 2?

☐ Yes – answer additional questions below

☒ No

If yes, answer the questions below:

Does this solution's new usage of data stay consistent with the existing purpose of the data shared?

☐ Yes ☐ No ☐ Unclear

For example, if full name and email address were initially collected to sign up for a Parks mailing list, a solution that sends the emails for this mailing list may be consistent with the existing purpose. However, using the data for a different mailing list would be inconsistent and require an updated privacy notice to the data subjects (e.g., the individuals who provided their full name and email address).

Attach the Privacy Notice which details the existing purpose and usage of the data shared.

☒ Attached ☐ Could not locate notice or notice does not exist

If Notice is not attached, please provide detail (if available) about the existing purpose, data usage and Privacy Notice below:

Vigilant Solutions acknowledgement banner.

Disclosure (CA) - Intended Use of LPR Data

Each Authorized User agrees that scanned plate, hotlist information, and networking resources are to be used solely for law enforcement purposes only and consistent with the law.

Authorized Users shall not use or share the information for any unethical, illegal, criminal, or commercial purpose.

Pursuant to California Government Code Section 3, Chapter 17.25 (commencing with section 7284) federal, state, or local law enforcement agencies **shall not use any non-criminal history information contained within the database for immigration enforcementpurposes.** This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. sections 1373 and 1644.

Attach the additional or updated Privacy Notice which details the new purpose of the data used in this solution

☐ Attached ☐ Could not locate notice or notice does not exist

If Notice is not attached, please provide detail (if available) about the new purpose, data usage and Privacy Notice below:

Section 4

If collecting new information, either directly or through another department or non-City entity, answer the following:

Will the data subject (individual which is the focus of the data collected) be provided a Privacy Notice upon collection?

☐ Yes ☒ No

Will the data subject be required to give “express consent” for the data collected?

☐ Yes ☒ No

Note: “Express consent” differs from a Notice in that for consent a data subject must explicitly agree (usually in writing) to the data usage outlined in the Notice. This can be done via a signature, a check box online, or other explicit method. Providing Notice only requires that the Notice be easily accessible to the data subject, and the data subject is made aware of the Notice and given the opportunity to read the Notice before data collection

If the data subject is not provided a Notice before data collection, explain why below. For example, is the data being collected as part of an arrest, or an emergency response?

License plate images are collected by commercial entities driving on public roads.

Attach the Privacy Notice which details the purpose of the collected data used in this solution

☐ Attached ☐ Could not locate notice or notice does not exist

If Notice is not attached, please provide detail (if available) about the purpose, data usage and Privacy Notice below:

Privacy review: Filled out by Digital Privacy Office

The San José Police Department is purchasing continued access to a commercial database of license plates. No new data is being collected and no new data is being added to the database by the City of San José. Data provided to the Police Department is limited to license plate numbers, locations, and pictures thereof for the purposes of identifying the location of a vehicle.

Recoverable Signature

X Albert Gehami

Albert Gehami
Digital Privacy Officer
Signed by: 435f4c7e-2188-440c-8663-ca37a7a0da8d