

Privacy procurement form (Beta v0.1)

Fill out the form below when seeking procurement of a product, service, or other 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, please 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 procurement

Name (first and last): [REDACTED]

Department: Human Resources

Title: Analyst II

Email: [REDACTED]

Phone: [REDACTED]

Summarize the purpose of the data solution below:

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

This data solution is meant to inform performance measure generation, tracking monthly changes in performance metrics, monitoring the health of public metrics, and generating visuals for the public to understand the story behind the data.

Where is the data used originating? Mark all that apply

Public data sources (e.g., US Census, CDC, any data readily accessible online) – if all data is from public sources then you do not need to complete any other portion of this form

Private data collected on exclusively on City employees and programs – fill out Section 2

Private data (existing data not public) shared **from** a non-City entity (e.g., a 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), detail which of the following Personally Identifiable Information (PII) this solution uses:

PII category of information

Category of PII	Sub-categories
<input type="checkbox"/> Personal Data	<input type="checkbox"/> Full name; <input type="checkbox"/> Home address; <input type="checkbox"/> Email address; <input type="checkbox"/> Phone, laptop, or other device IP ¹ address; <input type="checkbox"/> Government-Issued ID # (e.g., Driver’s License, Passport, Social Security Number); <input type="checkbox"/> Employee ID number; <input type="checkbox"/> License Plate <input type="checkbox"/> Credit or debit card information; <input type="checkbox"/> Bank account, brokerage account or other financial information; <input type="checkbox"/> Date of birth; <input type="checkbox"/> Place of birth; <input type="checkbox"/> Other written or scanned information that can directly tie to an individual or household
<input type="checkbox"/> Sensitive PII or demographic-related PII	<input type="checkbox"/> Biometric data; <input type="checkbox"/> Genetic data; <input type="checkbox"/> Physical identifiable characteristics; <input type="checkbox"/> Other health records <input type="checkbox"/> Race or ethnic origin; <input type="checkbox"/> Nationality; <input type="checkbox"/> Immigration status; <input type="checkbox"/> Religious affiliation; <input type="checkbox"/> Political affiliation; <input type="checkbox"/> Education records <input type="checkbox"/> Criminal records <input type="checkbox"/> Other sensitive written or scanned information traditionally kept confidential
<input type="checkbox"/> Image data	<input type="checkbox"/> Picture that can identify an individual by their face or other physical and contextual information ²
<input type="checkbox"/> Recording data	<input type="checkbox"/> Video that can identify an individual by their face or other physical and contextual information; <input type="checkbox"/> Audio that can identify an individual by their voice or other contextual information
<input type="checkbox"/> Geolocation data	<input type="checkbox"/> Data affiliated with a vehicle, computer, or other device that can be used to identify an individual’s physical location
<input type="checkbox"/> Other private or personal information	<i>Detail other private or personal information that does not fit into the categories above:</i>

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

² 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 PII (i.e., non-public data that fits into one of the categories above) shared from or to another department or non-City entity, answer the following:

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:

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 PII, 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?

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

This project compiles a database of public information to measure aggregate health outcomes. All information used is already publicly available, so it presents no privacy concern. Approved from Privacy.

 Recoverable Signature

X Albert Gehami

Albert Gehami

Digital Privacy Officer

Signed by: 435f4c7e-2188-440c-8663-ca37a7a0da8d