

Privacy initiative and procurement form

Fill out this form 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”).

For support and questions, contact the Digital Privacy Officer at digitalprivacy@sanjoseca.gov. Once completed, email this form to the Digital Privacy Officer or respond to the requestor.

NOTE: An anonymized version of this document (removing contact and other personal information) may be readily available to the public on San José’s Digital Privacy webpage.¹

Section 1

Main point of contact for solution

Name (first and last):

Department: City Manager’s Office

Title: Senior Executive Analyst

Email:

Phone:

Summarize the project below and how it uses data:

This should be a 1-3 sentence summary of the project. Further detail can be provided in Section 2 if required.

Create a public mapping tool of restaurants that represent food from different countries around the world in San Jose in order to highlight the diversity and contributions of immigrants past and present. All information found on the map can be obtained by google such as the name of the restaurant, the address, and the type of food they serve.

Where is the data used originating? Mark all that apply by highlighting the in red

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

¹ Sanjoseca.gov/digitalprivacy

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 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 on the following page)
- No

If sharing data publicly, is there an underlying dataset which includes PII that is directly linked to the data shared?

For example, this [public map shows crimes in the 95113 zip code](#). However, the underlying data is anonymized before it is uploaded (names removed, location is connected to a City block, etc.) and if a hacker were to access the back-end of the website, they would only find the anonymized data.

- Yes (mark the relevant PII categories and sub-categories below)
- No
- N/A – data is not shared publicly
- Uncertain (contact the Digital Privacy Officer to discuss)

Detail which of the following Personally Identifiable Information (PII) this solution uses, mark all categories and subcategories that apply by highlighting the in red:

Category of PII	Sub-categories
<input type="checkbox"/> Personal Data	<p>General: <input type="checkbox"/> Full name; <input type="checkbox"/> Home address; <input type="checkbox"/> Date of birth; <input type="checkbox"/> Place of birth</p> <p>Technology: <input type="checkbox"/> Email address; <input type="checkbox"/> Phone, laptop, or other device IP² address; <input type="checkbox"/> Vehicle make, model and year</p> <p>Government-issued ID: <input type="checkbox"/> Driver’s License; <input type="checkbox"/> Passport; <input type="checkbox"/> Social Security Number; <input type="checkbox"/> Federal Employer ID or Tax ID; <input type="checkbox"/> Employee ID number; <input type="checkbox"/> License Plate</p> <p>Financial data: <input type="checkbox"/> Credit or debit card information; <input type="checkbox"/> Bank account, brokerage account or other financial information</p> <p><input type="checkbox"/> Other written or scanned information that can directly tie to an individual or household – detail below:</p>
<input type="checkbox"/> Sensitive PII or demographic-related PII	<p>Health data: <input type="checkbox"/> Biometric data; <input type="checkbox"/> Genetic data; <input type="checkbox"/> Physical identifiable characteristics; <input type="checkbox"/> Other health records</p> <p>Race/Ethnicity: <input type="checkbox"/> Race or ethnic origin; <input type="checkbox"/> Nationality; <input type="checkbox"/> Immigration status</p> <p>Religion/Politics: <input type="checkbox"/> Religious affiliation; <input type="checkbox"/> Political affiliation; <input type="checkbox"/> Voter status</p> <p>Sensitive personal records: <input type="checkbox"/> Education records; <input type="checkbox"/> Criminal records</p> <p><input type="checkbox"/> Other sensitive written or scanned information traditionally kept confidential – detail below:</p> <p>NOTE: Do not mark if data is only shared/collected/used in aggregate of a population larger than 1,000³ (e.g., # of registered voters in San José)</p>
<input type="checkbox"/> Image data	<input type="checkbox"/> Picture that can identify an individual by their face or other physical and contextual information ⁴ - detail below:
<input type="checkbox"/> Recording data	<input type="checkbox"/> Video that can identify an individual by their face or other physical and contextual information – detail below: <p><input type="checkbox"/> Audio that can identify an individual by their voice or other contextual information – detail below:</p>
<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 – detail below:
<input type="checkbox"/> Other private or personal information	<i>Detail other data that could directly or indirectly identify an individual:</i>

² Internet Protocol - An IP address is a unique address that identifies a device on the internet or a local network

³ 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](#)

⁴ An example of “contextual information” being used to identify someone could include a picture of a license plate, car make model and year, or a picture of someone’s backside next to a house with a visible address.

Project context and purpose:

What is the issue this project is looking to address? What is the question this project is trying to answer? What is the opportunity or new benefit this project is meant to create?

The project is looking to highlight the diversity and contributions of our immigrant community, those who have been here for generations and those who have newly arrived, through the representation of food. This project will indirectly also benefit small local businesses who have struggled through the pandemic and highlight restaurants that many may have never known about.

Data collected/shared:

Summarize what data is being collected. This should include the Personally Identifiable Information categories that you marked in the table above.

Data that will be collected and shared can all be found on google, most often by the restaurant's own website. We will be collecting the name of the restaurant, the address, the country the food is representing, and whether they serve breakfast, lunch or dinner.

Data Usage:

How will the data be used? What are the usage limitations? Will this data regularly be used for law enforcement purposes, or will it only be used for law enforcement purposes when required by law?

The data will be used as a tool for residents to explore the diversity of San Jose's restaurant scene. The data will not be used for law enforcement purposes.

Data Retention:

How long will the data be kept? What relevant policies (e.g., laws, statutes, our City Retention Schedule) inform retention?

The data will be kept until the project is no longer beneficial or until it cannot be maintained any longer.

Access to the data:

*Who will be able to access the personal information collected? Mark all that apply by highlighting the **in red**.*

City staff

Third parties (list parties below, and explain how vendors or other partners can access and use the data):

General public (excluding via a Public Records Act Request)

(Data collected is not personal information but city staff and public have access)

How can data subjects (those who are the subject of the data collected) access their information to edit or correct it? Explain below:

We will be incorporating a webform that will allow restaurants to opt in to being listed on the map and editing their data.

Notice:

How will individuals be notified 1) that their data is being collected and 2) how their data will be used?

N/A

Selling data:

Will any of the information be sold by the City or a third-party? Projects that involve the selling of information will be rejected.

Yes

No

Section 3

If using private data shared from or to a 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 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 (data subjects would be the individuals who provided their full name and email address).

Attach the policy and/or data sharing agreement which details the existing purpose and usage of the data shared.

Attached Could not locate policy or policy does not exist

If policy is not attached, provide detail (if available) about the existing purpose, data usage and data sharing agreement below:

If data is being used for a new purpose, attach the policy and/or data sharing agreement which details the new purpose of the data used in this solution

Attached Could not locate policy or policy 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 (see definition of privacy notice below)?

Yes No

Note: A privacy notice should inform the individual of what is being collected, how it will be used, who can access it, how long it will be stored, and who they can contact for further information or to request edits to their data. Often this information is covered in the terms and conditions. Limited notices such as street signs may only provide some of this information upon collection, but all this information should be available somewhere, such as on the City website.

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

Yes No

Note: “Express consent” requires a data subject to 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 (a digital copy or a scan/photo of a physical copy) that will be provided to the individual upon collection.

Attached Could not locate notice or notice does not exist

If notice is not attached but still provided, 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 restaurants run/owned by immigrants in San José. 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