Privacy initiative and procurement form (v2)

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): Amory Brandt

Department: ITD

Title: Products, Projects Manager

Email: amory.brandt@sanjoseca.gov

Phone: 408-535-3565

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.

Public Portal/SJ Permits V2.1 (PP2.1) online permitting portal is an expansion of Public Portal V2.0, which will provide additional online permitting features to customers. As a result of PP2.1 implementation, customers (homeowners/property owners and business owners/contractors) will be able to apply for most permits online without the paper application process; navigate to the SJePlans (ProjectDox) portal; track the status of their plan review; estimate permit fees; and use an application "wizard" that will guide applicants through the permit type selection process.

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

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

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

☐ City staff

☐ Third parties (list below):

☐ General public (excluding via a Public Records Act Request)

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
☐ Personal Data	**General:** ☐ Full name; ☐ Home address; ☐ Date of birth; ☐ Place of birth **Technology:** ☐ Email address; ☐ Phone, laptop, or other device IP[1] address; ☐ Vehicle make, model and year **Government-issued ID:** ☐ Driver's License; ☐ Passport; ☐ Social Security Number; ☐ Federal Employer ID or Tax ID; ☐ Employee ID number; ☐ License Plate **Financial data:** ☐ Credit or debit card information - card numbers and payments are handled by a secure third party payment company; ☐ Bank account, brokerage account or other financial information ☐ **Other** written or scanned information that can directly tie to an individual or household – detail below:
☐ Sensitive PII or demographic-related PII	**Health data:** ☐ Biometric data; ☐ Genetic data; ☐ Physical identifiable characteristics; ☐ Other health records **Race/Ethnicity:** ☐ Race or ethnic origin; ☐ Nationality; ☐ Immigration status **Religion/Politics:** ☐ Religious affiliation; ☐ Political affiliation; ☐ Voter status **Sensitive personal records:** ☐ Education records; ☐ Criminal records ☐ **Other** sensitive written or scanned information traditionally kept confidential – detail below: **NOTE:** Do not mark if data is only shared/collected/used in aggregate of a population larger than 1,000[2] (e.g., # of registered voters in San José)
☐ Image data	☐ Picture that can identify an individual by their face or other physical and contextual information[3] - detail below:
☐ Recording data	☐ Video that can identify an individual by their face or other physical and contextual information – detail below: ☐ Audio that can identify an individual by their voice or other contextual information – detail below:
☐ Geolocation data	☐ Data affiliated with a vehicle, computer, or other device that can be used to identify an individual's physical location – detail below:

[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, car make model and year, or a picture of someone's backside next to a house with a visible address.

Category of PII	Sub-categories
☐ Other private or personal information	*Detail other data that could directly or indirectly identify an individual:*

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?

SJPermits is an online platform for residents, developers, architects, etc. to apply for permits which offers a self-serve and digital experience. The new release of SJPermits (V 2.1) will expand existing features within the online permitting system for customers. The most notable new feature includes the ability to apply for many additional permit types online instead of submitting a paper application. The SJPermits enhancements with V2.1 are expected to increase digitization of the permitting process, and increase access to the permitting process by providing services online.

Data collected/shared:

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

Applicant first and last name, e-mail, phone number, mailing address, and address or APN of the property that the applicant needs the permit for.

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 PII data will be used to contact applicants as needed to process their permit application. Inspection notices, soil reports, issued permits, etc. which contain the applicant and/or the property owner's name and mailing address are available publicly online.

https://portal.sanjoseca.gov/deployed/sfjsp

Data Retention:

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

Permitting records are kept permanently.

Access to the data:

Who will have access to the data? Is it just City departments, or will vendors or other partners have access? Who can access the data to edit or correct information?

City staff and vendors who complete software development on the platform have access to data, along with members of the public for select files (See link below)

https://portal.sanjoseca.gov/deployed/sfjsp

As required in the public record, members of the public will be able to access PII of property owners (their names and mailing addresses) which confirms who owns which properties and who is applying for any associated building permits.

Notice:

How will individuals be notified that their data is being collected and how it will be used?

The notice below will be added to the create account page

"This data is being collected and stored by City of San Jose in accordance with the City of San Jose E-Governance Policy."

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 (data subjects would be 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 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

The notice below will be added to the create account page on SJPermits,

"This data is being collected and stored by City of San Jose in accordance with the City of San Jose E-Governance Policy."

Note: The notice should inform the individual 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 for requesting edits to their data. Often this is covered in the terms and conditions.

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?

The applicant name, mailing address, property owner, and address of the property that the permit is being applied for are available on the public record.

https://portal.sanjoseca.gov/deployed/sfjsp

Attach the Privacy Notice (a digital copy or a scan 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, please provide detail (if available) about the purpose, data usage and Privacy Notice below:

Digital Privacy Office review

Summary – This project presents low-mid privacy risk and high civic value. Approved.

Notice – Notice is provided upon signing up and available on the side-bar of the site. To notify applicants that their personal information will be stored by the City, the following wording will be added to the create account page: “This data is being collected and stored by the City of San Jose in accordance with the City of San Jose E-Governance Policy.”

Minimization - The following project only requires necessary PII to provide the required services, which includes contact information to notify applicants about their building application, address of the relevant building, and names of inspectors, property owners, and other relevant parties required for public record purposes (such as identifying who legally owns a home).

Retention – Defined

Accuracy – users can update and correct their information online

Accountability – Data is securely stored with the City. Credit card payments are processed through an external secure vendor. The City does not store credit card information from payments on this platform.

Sharing – Some information is accessible to the public per public record requirements, otherwise data is kept within the City and trusted vendors as needed to provide the services

Equity - While home ownership and city land development has a racialized history, these broader issues are better addressed in Council and City policy than in a public works application portal.