DataSF Guides:

Department Guide to Personal Data Requests

A product of Datasf.org
City and County of San Francisco
Last revised: July 28, 2016

Table of Contents

In brief – what is this guide?

Chapter 22D "Open Data Policy" of the San Francisco Administrative Code requires that the Chief Data Officer "establish a process for providing citizens with secure access to their private data held by the City." (S.F. Admin. Code § 22D.2(b)(9).) This guide contains recommended processes for City and County of San Francisco (CCSF) departments and agencies (herein referred to as "departments") to:

1. Identify what, if any, private data about individuals (referred to herein as "personal data") they currently hold in an electronic, searchable database; and
2. Provide individuals with secure access to such data and/or ensure individuals can have secure access to such data in the development of future databases.

This guide will be periodically revisited and updated to take into account, among other factors, changes to the City's data policies, processes and systems.

NOTE: This guide is intended to implement the mandate in Chapter 22D that the City develop a strategy for the release of City-held personal data directly back to individuals who request such data. **This guide does not apply to requests for public records under the California Public Records Act or the Sunshine Ordinance. Departments should continue to follow their existing processes when responding to public records requests.**

Who is this guide for?

This guide is for departments. It contains guidance and options to allow departments sufficient flexibility to implement a process suited to their needs while ensuring individuals have secure access to their personal data held by CCSF. Since every department may have different legal requirements that apply to the data they maintain, the department should consult their assigned deputy city attorney about any special privacy requirements or restrictions that apply to their disclosure of personal data.

What is personal data?

Federal, state and City law all define different types of data as "private." For example, Chapter 12M of the San Francisco Administrative Code defines "Private Information" as "any information that (1) could be used to identify an individual, including without limitation name, address, social security number, medical information, financial information, date and location of birth, and names of relatives; or (2) the law forbids any person from disclosing."

For purposes of this guide, we will refer to private data about individuals as "personal data." Chapter 12M's definition does not encompass the entire universe of personal data. For certain types of personal data (*including but not limited to* health records, criminal justice records, Social Security number), federal and state law may govern the circumstances under which a person has a right to access his or her personal data. **Consult the City Attorney's Office about any special privacy requirements or restrictions on your department's disclosure of personal data to the individual it concerns.**

 **STOP: If your department does <u>not</u> hold any personal data, this guidance does not apply to you.**

What personal data must we provide under Chapter 22D?

If you hold personal data in an electronic, searchable database, you must provide individuals with secure access to their personal data, subject to any prohibitions or restrictions on disclosure of personal data to the individual it concerns under applicable law. It is advisable to limit access only to records that are retrieved by an individual's name or personal identifier.

This guidance does <u>not</u> apply to:

- Information maintained in paper record form; and
- Information maintained in a non-searchable database.

If your department is contemplating the development of an electronic, searchable database that will hold personal data, you must ensure secure access to personal data can be provided in the future.

This guide applies **<u>only</u>** to the disclosure of personal data directly to the individual who requests his or her own data. It does not apply to information relating to other people, activities, events, nor does it apply to public records requests.

 **STOP: If your department does <u>not</u> hold any personal data in an electronic, searchable database and is <u>not</u> contemplating the development of any such future database, this guidance does not apply to you.**

What if my department already provides individuals with their personal data?

This guidance is not intended to replace existing policies and practices where departments already have processes in place for providing individuals with their personal data under other applicable federal, state or local law or regulation. For example, if the Department of Public Health already supplies individuals with their personal health information according to the Health Insurance Portability and Accountability Act, then they should continue to do so per existing practice.

How does a person make a request for his or her personal data under Chapter 22D?

Step 1: Inventory the types of personal data held by your department, noting which data is held in a searchable, electronic database. We recommend you make the inventory publicly available. As an example, see the San Francisco Public Library's Patron Privacy Inventory: http://sfpl.org/pdf/about/administration/privacyinventory.pdf

Step 2: Make publicly available (e.g. on your department's website) the procedures for a person to submit a request for his or her personal data under Chapter 22D. See Appendix A for a template.

Step 3: You can create a Personal Data Request Form and/or accept written requests. See Appendix B for a template. Standard forms can make it easier for you to recognize a personal data request and make it easier for the individual to include all the details you might need to locate the data they want. At a minimum, you should make available the categories of personal data held by your department, the information needed from the individual, the requirements for proof of identity, and where to direct a request. Some departments may already allow individuals to access and update their private personal data via an online portal with secure login. The City Attorney's Office should be consulted to ensure the account registration and login process allow for appropriate authentication of a person's identity. See below.

Should I require proof of identity? How?

Yes, you should require proof of identity from a requesting party. There are serious legal consequences under federal and state law for improper disclosure of personal data to third parties. Accordingly, it is critical that departments take adequate steps to verify the identity of the requestor.

At a minimum, you should require:

- The requesting party present in-person a government-issued photo id at the time they make the request; or
- Forms or written requests that are mailed or faxed must be notarized or include a signature under penalty of perjury (see Appendix A or B for the penalty of perjury statement).

If your department already allows individuals to access and update their personal data via an online portal, the level of identity verification you require should take into consideration the possible harm which inappropriate disclosure of the personal data could cause to the individual concerned, as well as the potential to expose the City to legal liability. **Please consult the City Attorney's Office regarding verification of identity with respect to online portals.**

How should I provide secure access to personal information under Chapter 22D?

You can print out the personal data and provide it in paper form to the requesting party in-person or via mail or facsimile.

 Please note that e-mail is **not** a secure means by which to transfer personal data.

If your department allows individuals to access and update their personal data via an online portal with login, **please consult the City Attorney's Office regarding secure access procedures.**

Can I ask for more information before responding to a personal data request?

Key Takeaway: Be reasonable about what you ask for.

You may need to ask for more information than is initially given in an individual's request to find the personal data covered by that request. For instance, if a person asserts that not all information about him or her was included in a response, it would be reasonable to ask for more details as to what type of personal data or the source of the information he or she believes is missing.

You should not ignore a request simply because you need more information from the person who made it. Ensure the person knows you need more information and tell them what details you need.

How long do I have to respond to a request?

Key Takeaway: Respond within a reasonable amount of time, and clearly communicate on timing.

As a general rule of thumb, you should respond to personal data requests no later than **60 calendar days** within receipt of a complete request. Requests that are readily answerable should be responded to in less time. You may extend the 60-day deadline if necessary to respond to more extensive or demanding requests, or based on factors such as the total number of requests the Department receives per month, the volume of personal data requested, staff time spent responding to requests, and available departmental resources.

You should make publicly available (and include on a Personal Data Request Form) the response period.

Can I charge a fee for dealing with a personal data request?

No, except where federal, state or local legislation authorizes a fee.

What about repeated requests?

Unless a reasonable interval – at a maximum 6 months – has elapsed between the first request and any subsequent ones, you are not obligated to respond to an identical request from the same requestor. If the information has been added to or amended since a previous request, you can provide only the new or updated personal data to the requesting party. If the data has not changed since the prior request, you can simply confirm that the prior response is still up-to-date.

Do I have to explain the contents of the information I send to the individual?

The information you provide should be in intelligible form. This means departments should make best efforts to explain any coded information; for example, through a table of definitions.

You should also provide to the individual the date on which you pulled the data.

What should I do if the data includes information about other people?

Where an individual's personal data appears alongside or combined with personal data of others, the data of such other persons should be removed or redacted from the records you produce. You should comply with the request only if there a way to segregate or redact the third parties' data, but not if such redaction/segregation is unreasonably burdensome**. You may, but are not required to, create a new document or data form in order to comply with the request.**

What about personal data held by my department that was received from a third party?

You should not refuse to provide personal data simply because you obtained that data from a third party. Instead, you must provide an individual with secure access to his or her personal data if it is held in an electronic, searchable database, save where prohibitions or restrictions on disclosure of the personal data to the individual it concerns exist under applicable law.

For example, if a department holds personal data in an electronic, searchable database that is received from various service providers and community based organizations, it should not refuse to provide this personal data simply because it was received from those third parties.

What about personal data requests made on behalf of others?

The individual seeking his/her personal data must submit the request themselves in order to ensure identity verification. Agents, attorneys or other representatives may not submit requests on behalf of individuals.

If I use a data processor, does this mean they would have to deal with any personal data requests I receive?

Responsibility for complying with a personal data request lies with you as the data steward.

Can I require an individual to make a personal data request?

No.

Appendix A: Website Template

What Personal Data [Department] Will Provide

[Department] will provide you with your personal data maintained in an electronic, searchable database that is retrieved by searching your name or personal identifier.

Types of Personal Data Maintained by [Department]

[Department] maintains the following personal data:

[Insert list]

Making a Request for Your Personal Data

1. Determine whether the personal data you are looking for is with **[Department]**. For more information on the types of records maintained by **[Department]**, go to **[Insert link]**.

   [*We recommend each department make publicly available an inventory of the personal data it holds in electronic, searchable databases. If your department does not have a publicly available inventory, delete the final sentence above.*]

2. **[*Departments to choose from the options below and delete those that are not applicable.*]**

   [Option 1:] Submit your request using the Personal Data Request Form, which can be found at **[Insert link]**. The form includes instructions.

   [Option 2:] You need not use a special form for making a request for your personal data. Please follow carefully the instructions below:

   a. You may use a plain sheet of paper or your letterhead.

   b. Write down what personal data you are looking for with as much detail as possible to help us locate it. Do not write your request in the form of a question, but clearly state what personal data you are requesting.

   c. Please provide the following information:
      i. Your full name, including distinguishing information (such as Dr., Jr., Sr., III), and any aliases or other names used (such as a maiden name);
      ii. Your present mailing address;
      iii. Your date and place of birth;
      iv. Types of personal data sought;
      v. Timeframe of record;

vi. Specific subject matter;
vii. The office(s) or program(s) originating or receiving the personal data;
viii. The particular event, policy, or circumstance that led to the entry of the personal data in **[Department's]** database;
ix. The reason you believe that the personal data exists within **[Department]** and not another government department or agency;
x. The statement in subsection (d) below, your signature, and the penalty of perjury statement per subsection (e) below; and
xi. Any other information that might help in identifying the personal data.

d. Let us know the address to which we should mail the response (will be sent via standard USPS) or the facsimile number to which we should fax it. [If you would prefer to pick it up in person, please provide an e-mail and phone number where we can reach you to notify you it is ready. Our offices are located at: **[Insert address]**.]

e. Include the following statement: "I am the individual who is the subject of the requested personal data."

f. Your signature must be dated and either notarized or submitted under penalty of perjury by adding the following **before** the signature:
   i. "I hereby declare that I am the person named below and I understand that any falsification of this statement is punishable under the laws of the State of California."

g. Send your request to the following:

   Address: **[Insert address]**
   Fax: **[Insert facsimile number]**

   Please write "Personal Data Request" on the envelope or the subject line of your fax.

[Option 3:] Log-in to the **[Insert name of portal]** at **[Insert link]** to retrieve[and update] your personal data.

[Determine your Fee Category]

[*Chapter 22M does not authorize a fee. However, departments may include information on fees if such fees are provided for by other applicable legislation*.]

What Happens Next After Making a Request

[*Include a brief description of the response period, any extension period and reasons for extension. Include contact information (if any)*.]

Appendix B: Personal Data Request Form

What Personal Data [Department] Will Provide

[Department] will provide you with your personal data maintained in an electronic, searchable database that is retrieved by searching your name or personal identifier.

Types of Personal Data Maintained by [Department]

You must determine whether the personal data you are looking for is with **[Department]**. **[Department]** maintains the following personal data: **[Insert list]**. [For more information on the types of records maintained by **[Department]**, go to **[Insert link]**.]

[Determine your Fee Category]

[*Chapter 22M does not authorize a fee. However, departments may include information on fees if such fees are provided for by other applicable legislation*.]

What Happens Next After Making a Request

[*Include a brief description of the response period, any extension period and reasons for extension. Include contact information (if any)*.]

APPLICANT INFORMATION (PLEASE PRINT OR TYPE)	
Name:	
Mailing address:	
Birth date:	
Place of birth:	

PERSONAL DATA REQUEST	
Personal data requested:	[Insert list of personal data held by department] □ [...] □ [...] □ [...] □ [...] □ Other _____
RESPONSE METHOD	
Please send my response:	□ To the mailing address above (will be sent via standard USPS) □ To the following mailing address: _____ □ To the following facsimile number: _____ □ [I will pick it up in person. When my request is complete, please notify me at: Phone #:_____ E-mail address:_____] [Insert office address for pick-up]

SWORN STATEMENT

I hereby declare under penalty of perjury that I am the person named below and I understand that any falsification of this statement is punishable under the laws of the State of California.

Subscribed to this _____ day of _____, 20___, at
(Day) (Month)

_____, _____.
(City) (State)

_____

PRINTED APPLICANT NAME

_____

SIGNATURE OF APPLICANT

CERTIFICATE OF ACKNOWLEDGEMENT

State of _____)

County of _____)

On _____ before me, _____, personally
(Date) (Name and title)

appeared, who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person executed the instrument. I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.
(Seal)

_____

SIGNATURE OF NOTARY PUBLIC