



PRIVACY FOR CHIEF DATA OFFICERS



CONTENTS

Acknowledgement and Introduction to Privacy for Chief Data Officers	3
Know your agency’s Senior Agency Official for Privacy (SAOP).	4
Become familiar with the agency privacy program.	4
Know the definition of personally identifiable information (PII).	4
Identify the data projects and initiatives in your office that involve data about people, including PII. Know what PII your agency collects already, especially if you are considering using such data for a project or program.	4
Know the data stewards at your agency, especially if their data is being used by your office on projects or programs (or being considered for use).	4
Work with the SAOP and agency privacy program to address privacy considerations at the earliest planning and development stages of agency data projects and initiatives, and continue to do so throughout the life cycle of the information.	5
To help facilitate such conversations between CDOs and SAOPs, consider these initial questions:	5

ACKNOWLEDGEMENT AND INTRODUCTION TO PRIVACY FOR CHIEF DATA OFFICERS

The FPC Data Driven Policy (DDP) working group, led by Eric Stein of the State Department under the guidance of the FPC Executive Committee, strives to enhance federal policy-making through innovative data use. This document was developed by the DDP to promote collaboration between agency Privacy Offices and Chief Data Offices. It does not constitute OMB guidance or policy.

[Executive Order 13719](#) established the [Federal Privacy Council \(FPC\)](#) on February 9, 2016. The FPC is the principal interagency forum to improve the privacy practices of agencies and entities acting on their behalf.

To help facilitate timely and effective coordination on privacy issues associated with data initiatives, the FPC developed this informational resource for Chief Data Officers (CDOs) at federal agencies to understand how their work fits with that of Senior Agency Officials for Privacy (SAOPs) and agency privacy programs. It suggests some initial starting points for those collaborative efforts.

FPC efforts are underway to have additional privacy resources for Evidence Act Council members, including an annual session where SAOPs and CDOs can collaborate on lessons learned and real-time challenges. Questions or ideas are welcome at privacy.council@gsa.gov.

Know your agency's Senior Agency Official for Privacy (SAOP).

- SAOPs have agency-wide responsibility and accountability for the [agency's privacy program](#). SAOPs are responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks.
- SAOPs and CDOs need to work together to address privacy issues associated with, or potentially associated with, data initiatives implicating privacy laws and policies, such as the Privacy Act and matching programs.
- The [Federal Privacy Council](#), reachable at privacy.council@gsa.gov, can help connect you with the SAOP.

Become familiar with the agency privacy program.

- Have you and your staff completed your agency's required privacy training?
- You can learn more about privacy programs by watching four short videos at <https://www.fpc.gov/learn-about-federal-privacy-program/>.

Know the definition of personally identifiable information (PII).

- As defined in [OMB Circular A-130, Managing Information as a Strategic Resource](#), PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information linked or linkable to a specific individual.

Identify the data projects and initiatives in your office that involve data about people, including PII. Know what PII your agency collects already, especially if you are considering using such data for a project or program.

- Privacy considerations may apply to a range of people who interact with agencies, including agency employees, contractors, grantees, students, U.S. citizens or Lawful Permanent Residents, non-citizens, and others.
- There are legal requirements for agencies handling information about people, as well as prohibitions on collecting this data outside of specific systems for official use. For example, there are specific requirements for handling records covered by the Privacy Act of 1974.

Know the data stewards at your agency, especially if their data is being used by your office on projects or programs (or being considered for use).

- Have you contacted the data stewards or custodians at your agency or otherwise, so they are aware of your intended use of the data?
- This outreach can help prevent challenges after CDO work has started.

Work with the SAOP and agency privacy program to address privacy considerations at the earliest planning and development stages of agency data projects and initiatives, and continue to do so throughout the life cycle of the information.

- Among other steps to ensure compliance and manage privacy risk, the SAOP and agency privacy program can work with you to apply the [Fair Information Practice Principles \(FIPPs\)](#), as articulated in OMB Circular A-130, when evaluating information systems, processes, programs, and activities that affect individual privacy.

To help facilitate such conversations between CDOs and SAOPs, consider these initial questions:

- What is the authority for collecting the information?
- What laws and policies govern the handling of this information?
 - Have you identified any relevant [system of records notices \(SORNs\)](#)? Is there a matching program?
 - Is there a relevant [privacy impact assessment \(PIA\)](#)?
 - If handling another agency's data, have you reviewed the Data Sharing Agreement, Memorandum of Agreement/Understanding (MOA/MOU), or Interagency Agreement (IAA) that governs access and use?
- Are you aware of the required safeguards and have you integrated the appropriate privacy controls into your information handling practices?
- What limitations are there on the use of the information?
- What is the end-to-end process by which this data will be used, disseminated, and stored?
- Will the data be tagged?
- What access controls will you employ? Role based? Attribute based?
- Do you know what you are required to do in the event of a breach or spillage of data? What about when your agency is not the steward or custodian of the data, or when there is a breach involving data, your agency shared with another party?
- What processes are in place to govern sharing data with third parties (e.g., other agencies, private companies, non-profits), including obtaining permission to share the data?
- What are your responsibilities and requirements for ensuring compliance with federal data security standards and practices for both your agency's own data and for data obtained from external sources?
- Have you considered how recipients of products with PII will store and safeguard any PII according to federal data security standards?