

Role of the Data Privacy Point of Contact

Each state agency is required by Ohio Revised Code 1347.15(B)(7) to appoint a Data Privacy Point of Contact (DPPOC):

[...] the director of the state agency [shall] designate an employee of the state agency to serve as the data privacy point of contact within the state agency to work with the chief privacy officer within the office of information technology to ensure that confidential personal information is properly protected and that the state agency complies with this section and rules adopted thereunder;

Who should be the DPPOC within your agency and what does the DPPOC do? Below are some answers to potential questions about the DPPOC position.

Your agency has to have one. Why not put it to good use?

Robust privacy practices build trust with customers and employees in addition to enhancing an agency's reputation. Good privacy is good government – no matter the nature of the agency. An internal privacy adviser, familiar with the business as well as with privacy law adds value to the agency and all of its components.

An empowered DPPOC can help prevent problems from arising. This saves expense and maintains the public's trust in the agency. If someone complains that the agency has breached their privacy, the DPPOC can handle things quickly and effectively. This is particularly important because agencies usually have an ongoing relationship with the person (for example, a customer or an employee). Again, this can save money and time. Thus, a privacy coordinator is not only required by law but an invaluable asset for agencies.

What does a DPPOC do?

A DPPOC:

- is familiar with any other legislation governing the agency's responsibilities and limits in regards to personal information;
- is familiar with Chapter 1347 of the Ohio Revised Code, "Personal Information Systems";
- works to address inquiries and complaints from the agency's clients about privacy matters;

- coordinates privacy impact assessments for the agency
- trains other staff at the agency on good privacy practices;
- advises managers on how to ensure the agency's business practices comply with privacy requirements;
- advises managers on the privacy impacts (if any) of changes to the agency's business practices and information systems;
- advises managers if improving privacy practices might improve the business;
- coordinates requests for access to personal information, or correction of personal information; and
- acts as a liaison for the agency with the State Chief Privacy Officer. This is particularly important if the agency is responding to a possible privacy breach. The Chief Privacy Officer also regularly e-mails the DPPOC network with privacy-related news and guidance.

Who should serve as the DPPOC?

The DPPOC is a multi-disciplinary role, and so a successful DPPOC needs to have the knowledge and capability to coordinate issues involving legal, IT and the business units. With regard to other key characteristics, a DPPOC is someone who:

- Understands the type of information the agency collects and it works with the agency's key business processes and systems;
- Understands the legal basis for the agency collecting, using and sharing personal information;
- Is capable enough with legal concepts to understand the privacy laws that regulate the agency;
- Has a degree of comfort with technology to understand how information is used and flows to, from and throughout the agency.
- Is sufficiently positioned to advocate appropriate solutions to address risks to individuals (harms from improper disclosure or use) and to the agency (lack of legal compliance and loss of public trust).
- Has support from senior leadership.

This depends on the size of the agency, the responsibilities of the agency, and the type of personal information it handles. For example:

- In a small agency, like a small business, the overall manager will often be responsible for legal compliance requirements, including privacy in addition to labor, equal opportunity, ethics, etc. An existing staff member might be asked to advise the manager or managers on privacy issues.
- If the agency has an in-house lawyer, that person is sometimes the DPPOC, particularly those agencies with significant privacy regulations.
- Sometimes, an agency IT administrator or information security officer will also serve as a data privacy point of contact.
- In large agencies or agencies that handle a lot of personal information, there may be a need for one or more employees focusing exclusively on privacy matters.

In the end specific qualifications do not matter as much as having a DPPOC upon whom other managers can rely as a resource for privacy issues.

Training and help for DPPOCs

The Office of Information Security and Privacy is available to assist DPPOCs.

- We offer privacy leadership training sessions each year.
- Our staff can answer general questions about how certain privacy laws work. We cannot provide legal advice on particular problems, but we may be able to suggest someone and resources that can help.
- **Communicate agency privacy concerns to the Chief Privacy Officer:** Please help ensure that the Chief Privacy Officer is aware of privacy-related issues within your agency. The Office of Information Security & Privacy has a number of resources that may help you address a privacy problem. Also, if a number of agencies experience the same problem, an opportunity for an enterprise approach may apply.
- **Please submit contact information for your agency data privacy point of contact to the Office of Information Security and Privacy.**

Contact us at chief.privacy.officer@oit.ohio.gov or (614) 387-0320 if you think we may be of assistance.