WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

2020 State Agency Privacy Assessment

Findings from the Office of Privacy and Data Protection's annual privacy assessment of state agencies.

Introduction

RCW 43.105.369 requires the Office of Privacy and Data Protection to conduct an annual privacy review of agency practices. The results help OPDP measure privacy maturity across state agencies and develop resources and trainings where they are most needed. The goal is to establish an understanding of current practices, not to measure compliance with specific laws or standards. Agency roles and privacy requirements vary and best practices for one organization may not apply to another.

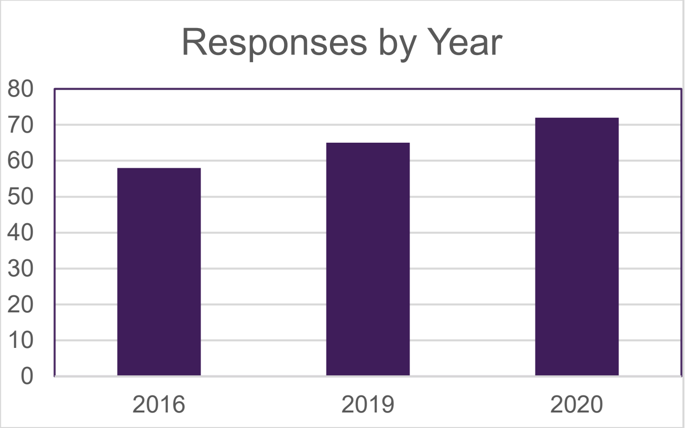
This assessment covers many of the basic components of a privacy program. To help all agencies gain a common understanding of the assessment and its purpose, OPDP held two sessions to walk through the material and answer questions.

The response rate has increased steadily since the assessment was introduced in 2016, with 72 agencies filling it out this year – a record number. Two-thirds reported that having strong privacy controls has become increasingly important during the past two years. No agencies said privacy became less important.

OPDP, overall, found that agencies are more likely to have core privacy program components – such as dedicated staff, formal policies and trainings – than in the past. However, significant gaps remain and even agencies with more privacy experience consistently indicate they need additional resources.

Participation and methodology

OPDP sent the assessment to 88 agencies as part of the Office of the Chief Information Officer (OCIO) 2020 Annual Certification. Including it in the annual certification helps OPDP meet its statutory requirement to integrate its efforts with the OCIO and also creates additional accountability for agencies to complete the assessment.


Responses by Year

As noted earlier, 72 agencies responded this year, representing an 82% response rate.[1]

Agencies that do not maintain personal information about Washington residents were required to submit a response but did not have to complete the entire assessment. Instead, they only needed to indicate they do not maintain personal information.

For the purpose of this report, personal information – also commonly referred to as personal data or personally identifiable information – is defined as information identifiable to a specific individual. Sixty-one of the 72 agencies that completed the assessment this year indicated they maintain personal information about Washington residents. The information in this report is based on their responses.

The assessment gathered information on nine topics:[2]

- Types of personal information.
- Privacy roles and staffing.
- Training and policies.
- Transparency.
- Individual participation.
- Accountability.
- Data sharing.
- Data inventory.
- Future planning.

Personal Information

Information about a person that is identifiable to that specific individual.

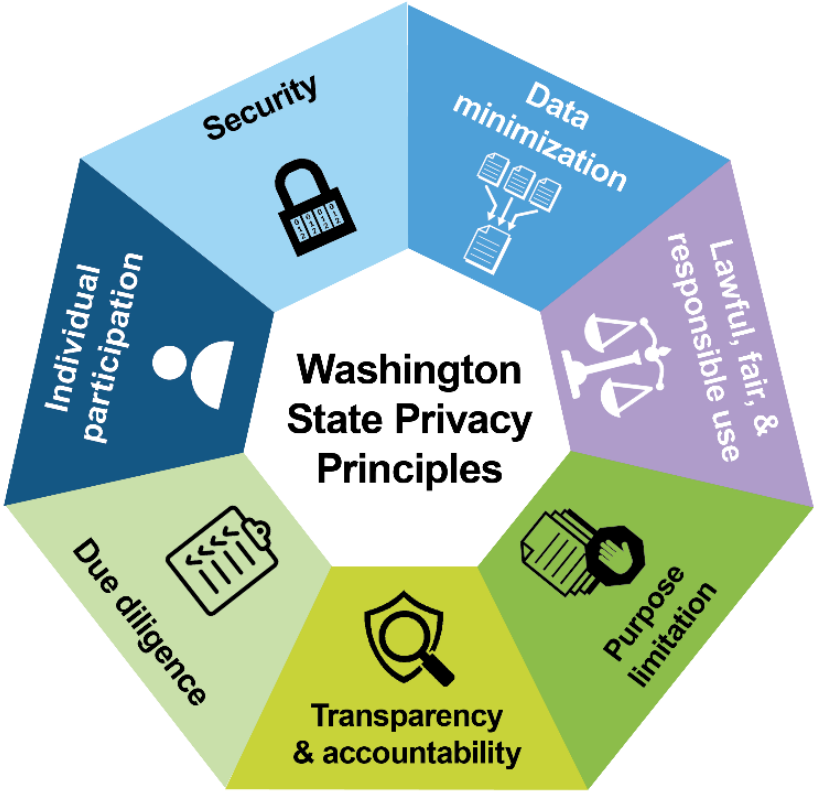
While the assessment helps gather valuable information about agency privacy protections, it is inherently quantitative. For example, it may measure whether an agency has formal policies and staff training but does not evaluate the accuracy and adequacy of the policies or measure the effectiveness of the training.

[1] This report includes information about responses submitted by November 16, 2020.
[2] A copy of the assessment is attached.

Privacy Principles

Several of the topics evaluated in the assessment closely align with the Washington State Agency Privacy Principles. These principles were finalized in October 2020 and this report makes those connections throughout.[3]

Privacy principles are a foundational element of any privacy program. Public agencies have an obligation to handle personal information about Washington residents responsibly and in a fair and transparent way. These fundamental privacy principles help to guide agency practices and establish public trust.


Washington State Privacy Principles
Security
Data minimization
Lawful, fair, & responsible use
Purpose limitation
Transparency & accountability
Due diligence
Individual participation

[3] A complete copy of the principles is attached.

PRIVACY PRINCIPLES	
LAWFUL, FAIR, AND RESPONSIBLE USE	Collection, use, and disclosure is: • Based on legal authority; • Not deceptive; • Not discriminatory or harmful; and • Relevant and reasonably necessary for legitimate purposes.
DATA MINIMIZATION	The minimum amount of information is collected, used, or disclosed to accomplish the stated purpose for collecting the information.
PURPOSE LIMITATION	The reasons for gathering information are identified before it is collected. Use and disclosure is limited to what is reasonably necessary in relation to the specific reasons the information was collected.
TRANSPARENCY & ACCOUNTABILITY	Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with and under what circumstances. Accountability means being responsible for following data privacy laws and principles.
DUE DILIGENCE	Taking reasonable steps and exercising care before and after entering into an agreement or arrangement with a third party that includes sharing personal information.
INDIVIDUAL PARTICIPATION	Give people control of their information when possible.
SECURITY	Appropriate administrative, technical, and physical security practices to protect the confidentiality, integrity, availability and control of personal information.

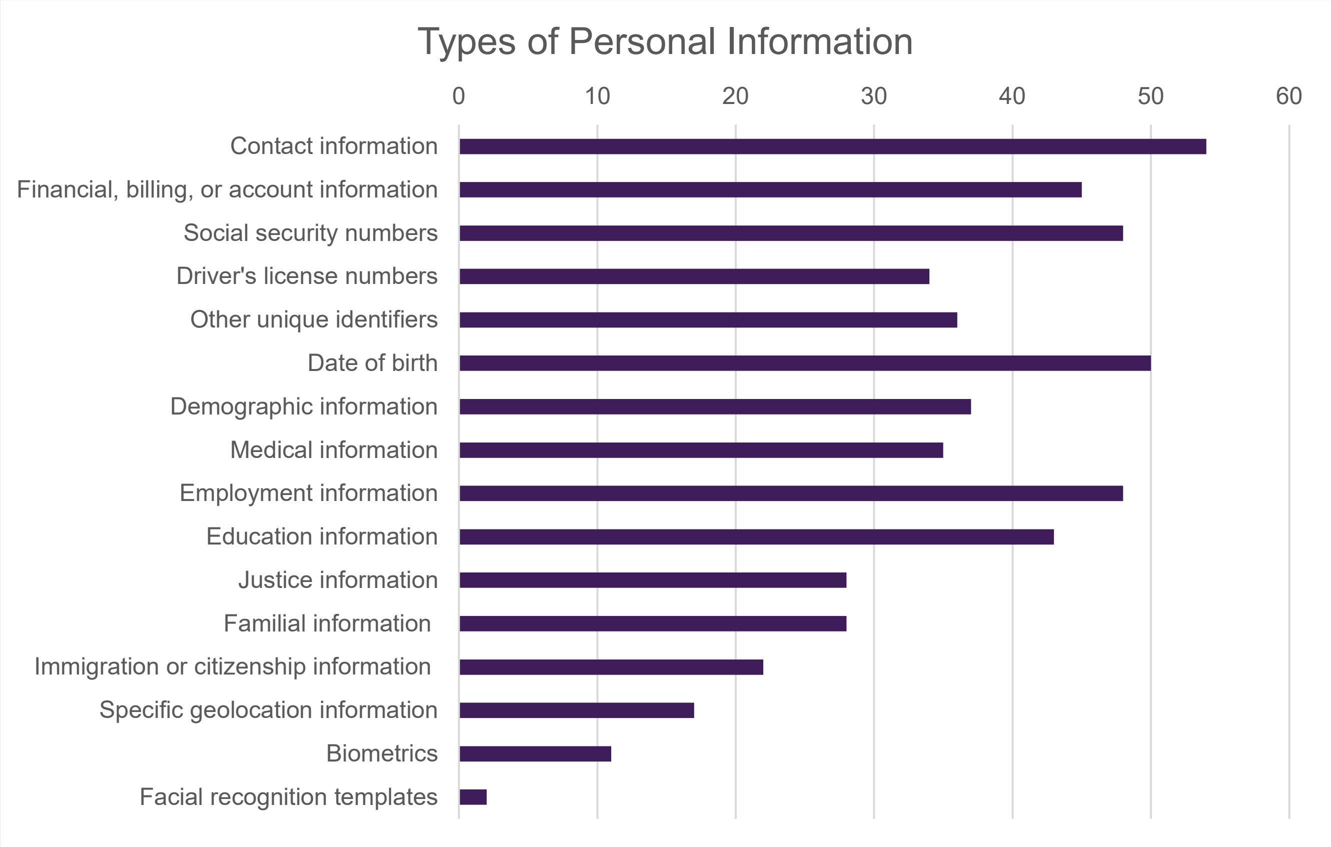
Types of personal information

The privacy assessment gathered information from agencies about the types of personal information they maintain and the sources for that information.

A broad range of data fits within the concept of personal information. It includes everything from basic contact information to social security numbers, detailed health information, immigration status and facial recognition templates. Different levels of protection are warranted for different types of information, depending on its sensitivity.

The types of information agencies have is one factor that can help determine the type of privacy controls needed to minimize risk and appropriately protect the information. Understanding what information an agency maintains is also essential to implement privacy principles like minimizing data and limiting uses.

The assessment revealed that many agencies maintain various types of sensitive personal information.



Privacy roles & staffing

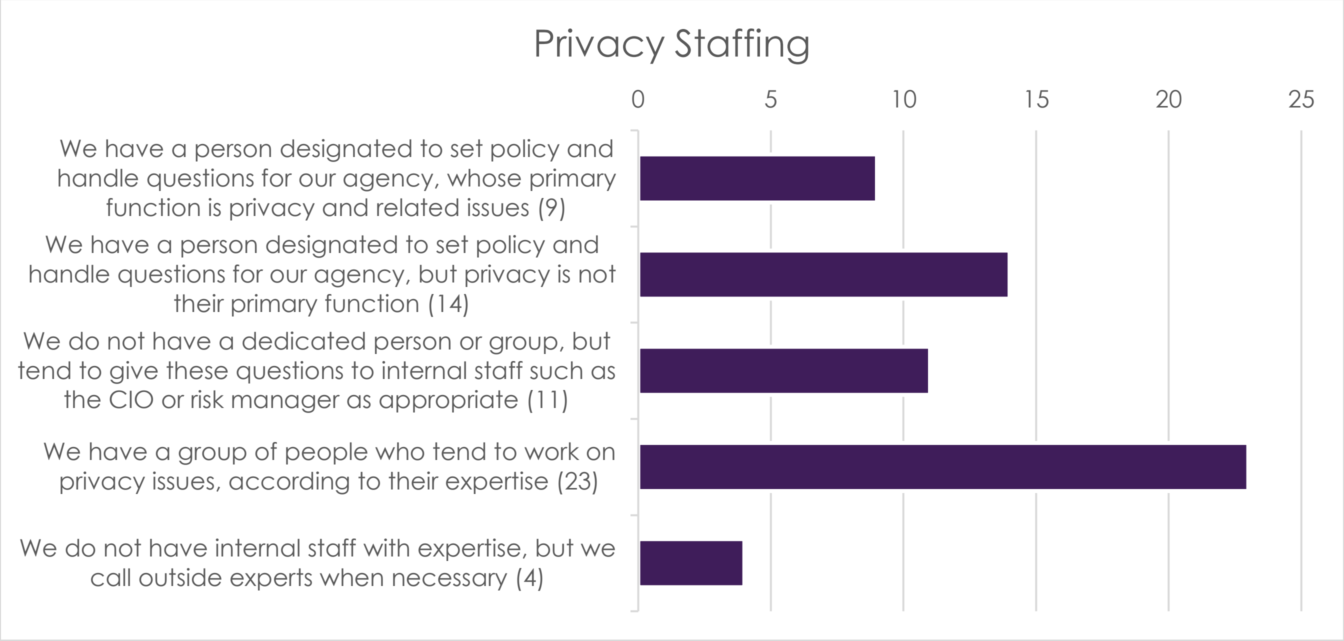
Agencies cannot adequately protect personal information without appropriate resources. The level of resources needed varies depending on the size of an agency, the functions it performs and the types and amount of personal information it maintains.

OPDP asked agencies to choose which of five potential staffing strategies best described their approach to privacy. The options ranged from having a designated person whose primary job is privacy, to contacting external resources such as the state Office of the Attorney General on an ad hoc basis.

Twenty-three agencies, 38% of those responding, reported having a specific person designated to handle policy and privacy questions. In 2019, only 13 agencies reported having a designated privacy officer. Nine agencies have a designated person's primary function is privacy and other related duties.

Having a designated person responsible for privacy is a significant step towards accountability. It is otherwise difficult for an agency to take on privacy initiatives and ensure privacy controls are being implemented across the agency.

Regardless of whether an agency has a designated person responsible for privacy, a variety of other staff tend to support privacy functions including information security staff, information governance staff, risk managers and records officers.



Training & policies

Privacy policies and staff training are both foundational controls.

Internal policies apply to how information is collected, used and shared. They demonstrate that an agency understands the protections that apply to its information and has implemented appropriate standards. They are one way to document the agency's commitments to how it will handle personal information.

Training helps ensure staff understand the importance of protecting personal information and know how to do it. Without training, staff may not understand the commitments the agency has made. This is particularly important when dealing with privacy because many agency employees may have access to personal information on a routine basis. They are the frontline when it comes to data protection. Taken together, clear policies and strong training are important pieces of the transparency and accountability privacy principle.

We asked agencies about three different types of privacy policies:

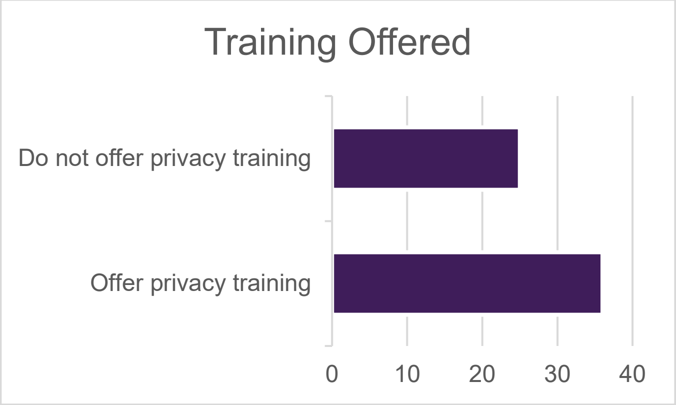
- Does your agency have formal privacy policies?
- Do those policies include a commitment to data minimization? Data minimization is a fundamental concept that applies to all agencies.
- Does your agency have formal policies or less formal standards that apply to subsets of particularly sensitive information or populations? Examples include information related to substance use disorder treatment and immigration. Having these types of policies or standards indicate privacy maturity. They show that an agency understands the level of protection needed will vary depending on the information maintained.

While most agencies have formal privacy policies, fewer have implemented data minimization policies or policies that contemplate varying levels of protection for different information.

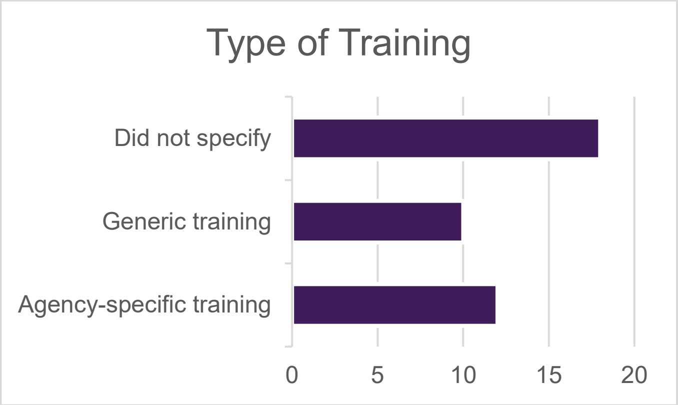
Formal privacy policies	**Data minimization policies**	**Particularly sensitive information policies**
With policies: 45	With policies: 30	With policies: 36
Without: 8	Without: 17	Agency standards, but no formal policies: 10
Other: 8 • Several agencies indicated policies are in development.	Other: 14 • Some indicated data minimization concepts are incorporated in other policies.	Agencies with no policies or standards: 14 • Eight agencies do not maintain particularly sensitive information.

We also asked agencies questions about training, including:

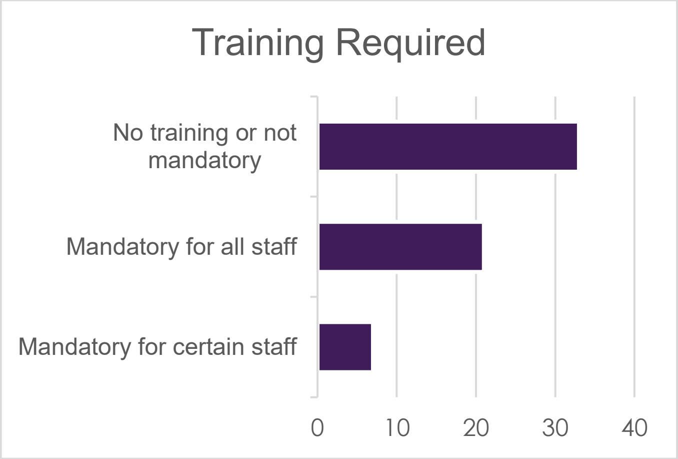
- Does your agency offer privacy training?
- Is the training mandatory? If so, is it mandatory for some or all staff?
- Is the training generic or specifically tailored to your agency?



Although most agencies have privacy policies, fewer offer training to staff. Approximately 59% of the agencies with personal information indicated they offer some type of privacy training.



Of the 36 agencies that offer training, 35% reported it is agency specific. Approximately 50% did not indicate if the training they offer is generic or agency specific. Agency-specific training takes resources to develop but helps ensure the training is matched to the types of information the agency maintains and the specific policies and procedures the agency has implemented.



Twenty-one agencies reported that privacy training is mandatory for all staff, and another seven reported that it is mandatory for certain staff.

Transparency

Agencies should be transparent about what information is collected, why, and who it is used by or shared with. This should be shared in a clear, honest and understandable way.

We asked agencies about two types of commonly used external-facing privacy policies. Depending on context and preference, a privacy policy might also be called a privacy notice, notice of privacy practices, privacy statement, or simply privacy information.

The first type of policy we asked about is a website privacy policy that addresses how information is gathered on the agency's website and how that information is used. This type of policy addresses topics like cookies and user tracking. Many agencies collect personal information in a variety of ways from a variety of sources, such as online portals, paper forms, in-person, other agencies, or other third parties. As a result, a website privacy policy covers just one piece of the information agencies have about Washington residents. Fifty agencies indicated they have this type of policy.

Next, we asked agencies whether they have a more general privacy policy that contemplates all the personal information the agency gathers from various sources. Typical information included in this type of notice includes at least:

- The types of information gathered.
- The purposes for which the information will be used.
- Who will use the information.
- How the information will be shared.
- An explanation of a person's ability to access or control their information.
- Who to contact with questions.

Thirty-two agencies, over half of the agencies with personal information, indicated they have this type of comprehensive privacy policy. Most agencies post it on their website, while some also mail the notice or provide it in-person.

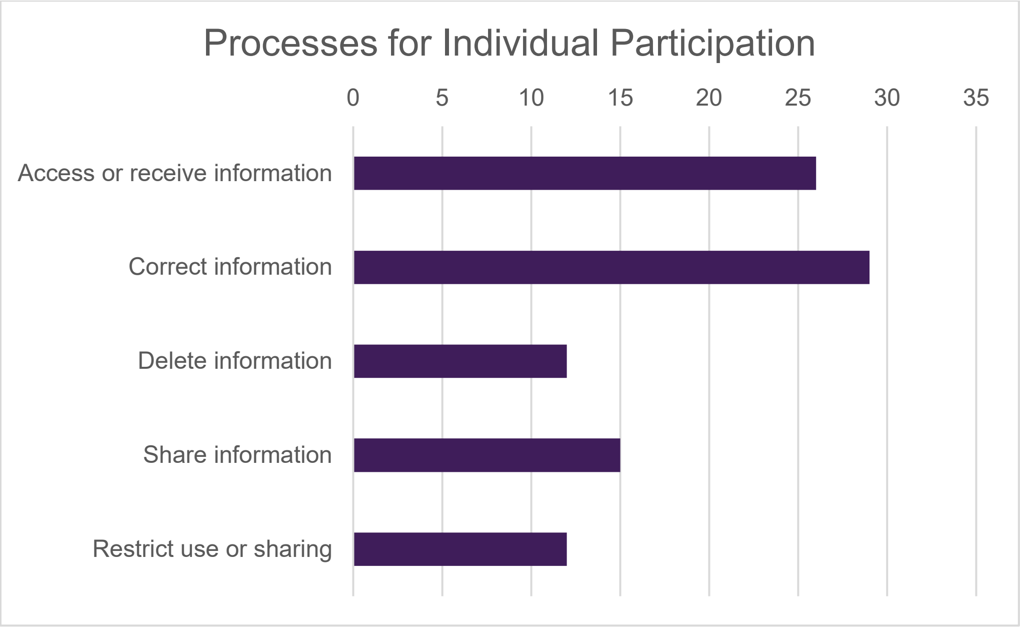
Individual participation

People should have control of their information when possible. This principle could be implemented by having processes for requests:

- To access or receive information.
- To correct information.
- To delete information.
- For information to be shared or sent to another person.
- For a restriction in how information is used or shared.

Because the government has a different relationship with Washington residents than a business has with a consumer, not all of these activities would be appropriate for all agencies or all government functions. Overall, 33 agencies indicated that they had at least one of these processes in place.

As shown in the chart below, agencies most commonly had a process for people to correct inaccurate information. Next most common is a process for people to access or receive information, which makes sense considering agencies' obligations under the Public Records Act.



Accountability

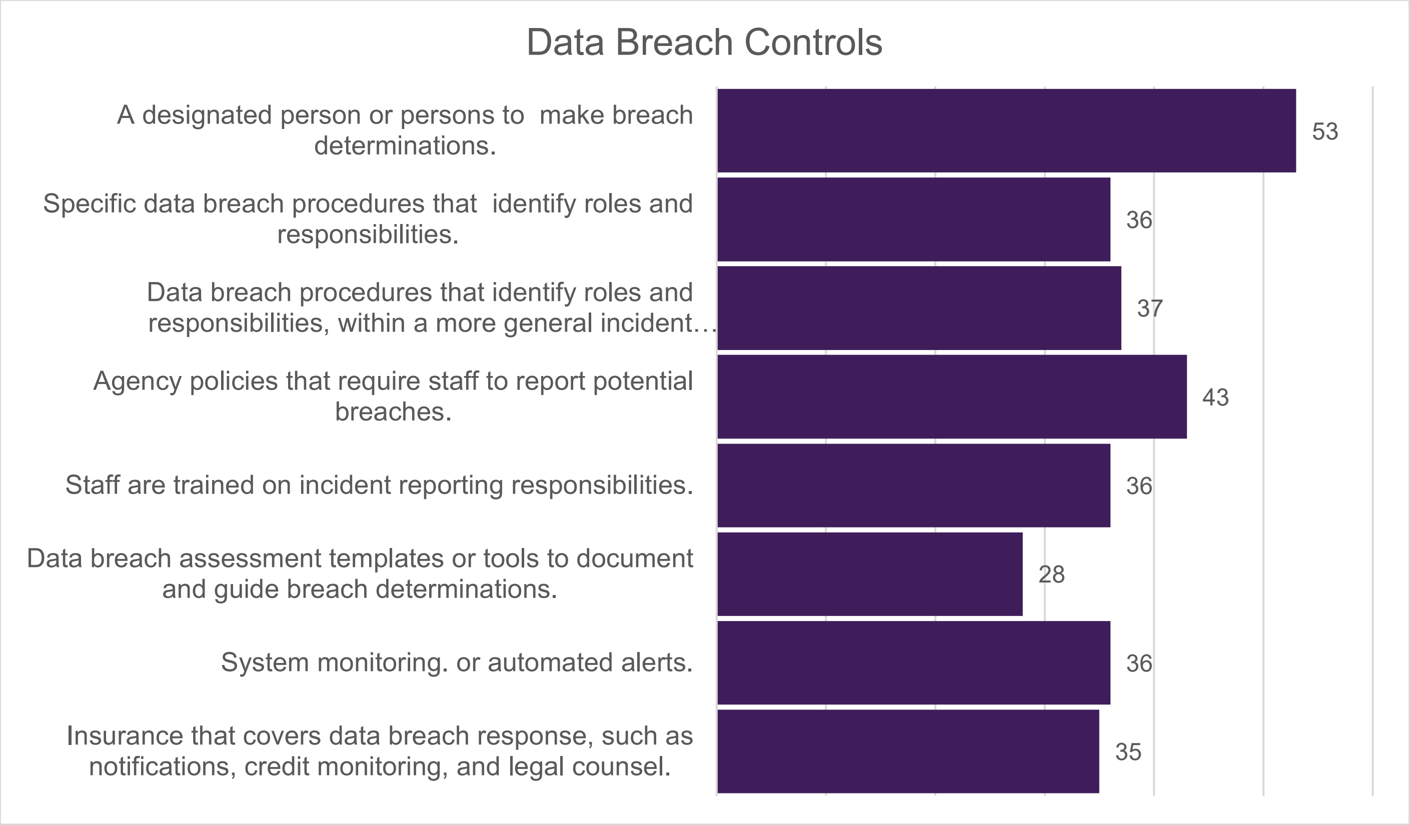
Accountability means being responsible and answerable for following data privacy laws and principles. It includes having appropriate policies and processes in place to detect unauthorized use or disclosure and notify affected individuals when appropriate.

We asked agencies about privacy incidents or breaches that occurred in the last year. An incident is the unauthorized use or disclosure of information, regardless of whether it requires notification under a breach notification law. A breach is an unauthorized use or disclosure that requires notification. Not all incidents are cybersecurity incidents. In fact, most are not. A privacy incident is often as simple as mailing information to the wrong person or disclosing information to an unauthorized person during a phone call.

The results from the assessment were similar to last year. Approximately the same number of agencies reported one or more incidents, and approximately the same number reported one or more breaches. The fact that incidents are detected and responded to is an indicator that appropriate controls are in place and staff understand how to identify and report them when there is an unauthorized use or disclosure. When an agency experiences no incidents, it could be a sign of excellent data protection and handling. It could also mean that incidents are going undetected due to inadequate controls.

87% of agencies reported they have one or more specific people designated to make breach determinations.

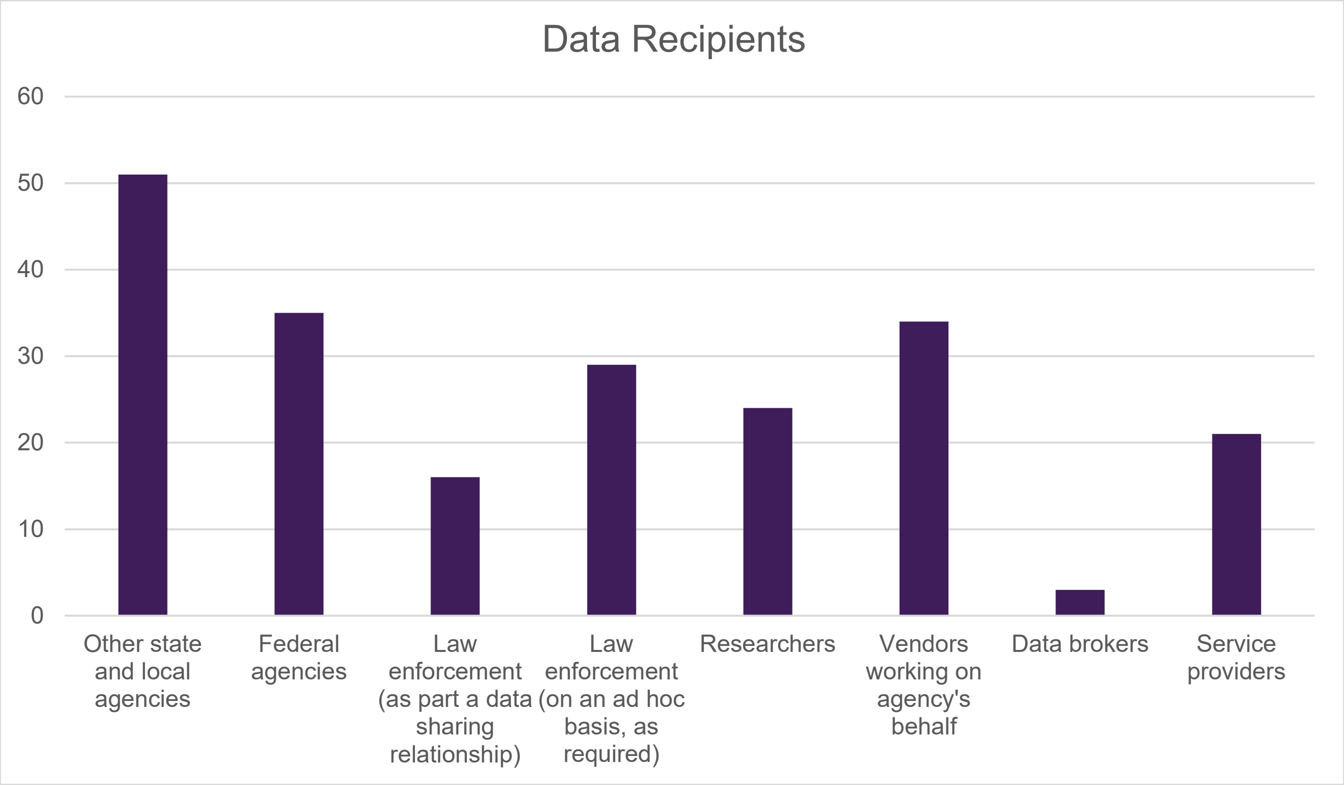
We asked agencies what steps they have taken to ensure incidents are discovered. Fifty-three agencies have designated at least one person to make breach determinations, but fewer than half have implemented assessment tools or templates.



For the first time, OPDP also asked agencies about incidents experienced by third parties they share information with. Third parties, such as service delivery providers, technology vendors and researchers, have significant access to personal information. Just as agencies must appropriately protect information they maintain they should also ensure third parties appropriately protect the information. Agencies were more likely to report that they experienced an incident or breach, than report that a third party experienced an incident or breach.

Data Sharing

In today's data-driven world, information is shared in a variety of ways. Agencies share information with each other, send information to federal agencies, support researchers, field requests from law enforcement and provide necessary access to a range of vendors and contractors. The chart below shows who agencies share information with. Notably, almost all agencies share information with other agencies. Only two agencies reported that they sell data as authorized by law.



This information sharing supports efficient and effective government, but agencies should exercise due diligence both before and after sharing information. Depending on context this may include taking steps like ensuring authority for the recipient to receive information, entering data share agreements with appropriate terms, and monitoring data protection practices.

- 46 agencies reported they have a review process to ensure contracting, privacy and security are considered before establishing a new data sharing relationship.
- 39 agencies have designated specific people to approve data sharing.
- 8 agencies have established a committee to review data share requests.

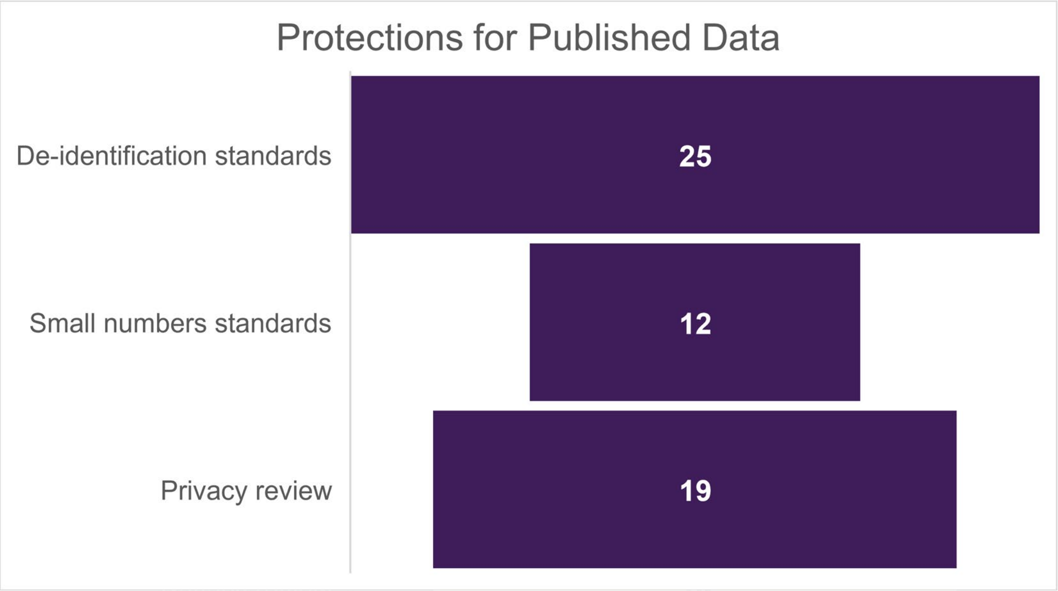
84% of agencies share personal information with other state or local agencies.

Having a committee to review data may not be appropriate for all agencies, but it can ensure appropriate vetting with a holistic view of an agency's data sharing relationships.

In addition to sharing personal information, agencies disclose information to remain transparent and accountable for government operations. These disclosures could include reports to the Legislature, publishing data on websites, or sharing analysis with stakeholders. These activities raise the possibility of disclosing identifiable information. Basic measures agencies can take to reduce the likelihood of published information being used to identify individuals include:

- **Creating de-identification standards**. De-identifying data is not as simple as removing obvious identifiers like names. Having established standards helps ensure appropriate and consistent practices.
- **Following a small numbers standard**. People can sometimes be re-identified when agencies release counts or aggregate information. That risk increases when the number of people with a specific characteristic, or the overall size of the measured population, decreases. Small numbers standards set a threshold size that counts must meet to be published. For example, an agency could decide that counts from 1-10 should not be published.
- **Privacy review of published datasets**. Even with appropriate standards in place, manual review helps identify risk with specific products. This is especially true when the context of the information is particularly sensitive.

Relatively few agencies have adopted these types of measures.

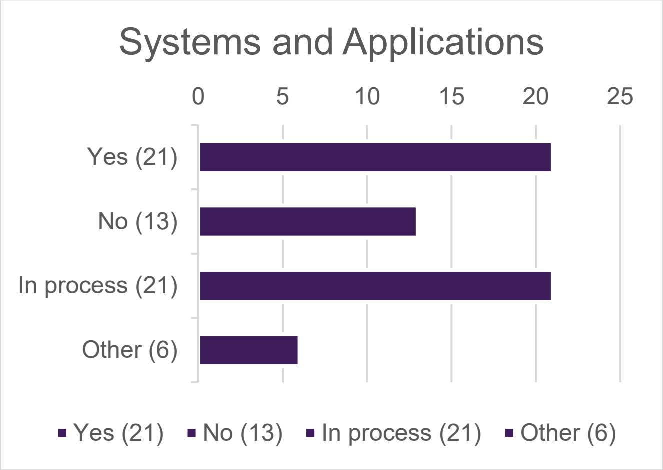


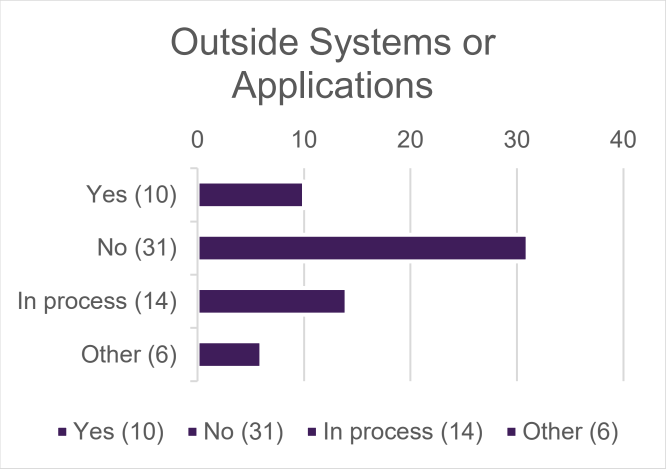
Data Inventory

Agencies often collect a variety of information from different sources and maintain it in numerous locations. Understanding where data is kept is critical to ensuring appropriate data protection measures. Without knowing what information is stored in a specific system, it is difficult to assess whether the agency is collecting the minimum amount of information necessary or tailoring the uses of that information to be consistent with the original reason for gathering the information.

We asked agencies if they had completed a data map or inventory of systems and applications that includes the type of personal information maintained. We also asked whether agencies have completed a data map or inventory that includes information stored *outside* of systems and applications. The question regarding outside systems or applications is necessary because information may never be added to a system or application or may be copied and saved somewhere else.

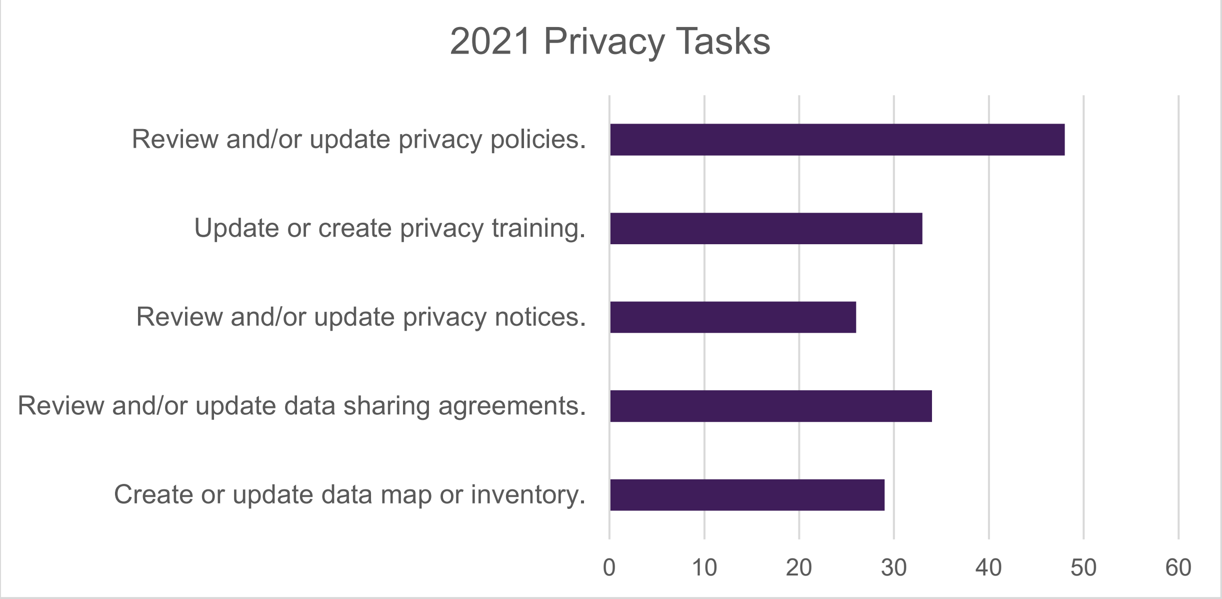
- 21 agencies indicated they had completed a data map or inventory of personal information in systems and applications.
- Another 21 agencies indicated they were in the process of completing one.
- Only 10 agencies had completed a data map or inventory that includes information stored outside systems or applications.





Future Planning

We asked agencies what privacy activities they already have planned for the next year, and what additional resources would be most helpful to their privacy posture. Most are planning to create or update one or more privacy fundamentals like policies, training or data maps.



Many agencies reported a need for additional funds to create or fill privacy positions. But they are also looking for additional resources that will help improve their privacy functions with existing funds. Many agencies indicated they would benefit from generic privacy training for staff. Others are looking for template privacy documents like data sharing agreements, privacy notices, policies, and position description forms.

Due to the range of functions performed by government agencies and the patchwork set of laws that apply to different agencies and types of information, one size fits all resources are not always appropriate. However, OPDP will continue to look for opportunities where these types of materials can benefit a large number of agencies with little customization required. For example, this year OPDP published a breach assessment tool that is appropriate for all agencies to use when evaluating incidents under the state's breach notification statute.

Conclusions and recommendations

Agencies hold a significant amount of sensitive information about Washington residents. This includes information about physical and mental health, substance use disorder, criminal justice, child welfare, education, immigration status, taxes and sensitive financial information. As awareness and concern about privacy continues to increase, many agencies are looking to improve their privacy practices.

The level of maturity varies – some are developing privacy practices for the first time while others are turning policies into programs or expanding existing programs. All agencies are looking for guidance and assistance. Providing the Office of Privacy and Data Protection the support needed to conduct additional outreach and create additional resources for state agencies will help ensure appropriate best practices to protect Washington residents' information.

The assessment revealed several measures some agencies can take to improve their privacy posture, including:

- **Designate a person or create a team in the agency to be responsible for privacy**. Even when their job is not solely privacy, this creates accountability, avoids silos for different privacy functions, and facilitates more contact with OPDP.
- **Provide more tailored training** that matches specific agency policies and applicable laws.
- **Adopt a breach assessment template and formal data incident response plan**. OPDP developed a template, which is available with related training on the OPDP website. Using a template helps ensure thorough and consistent assessment and creates a record of the agency's decision-making process regarding an incident.
- **Develop a data map or data inventory**. It is difficult to protect data and ensure proper data handling if an agency is not sure where the information is stored. Knowing the type of data that you collect, where it is held, with whom it is shared and how it is transferred is a central component of most data privacy and data security programs. The process of answering these questions is often referred to as a "data map" or a "data inventory."
- **Adopt standards for published data**. Privacy standards for information that is intended to be publicly disclosed helps avoid incidental disclosure and cultivate a culture of privacy.

We are encouraged by the steps agencies are taking to ensure they are appropriately protecting personal information. The OPDP is committed to collaborating with agencies and cultivating further growth in privacy and data protection.