WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Office of Privacy and Data Protection

2021 State Agency Privacy Assessment

Table of Contents

Introduction

RCW 43.105.369 requires the Office of Privacy and Data Protection (OPDP) to conduct an annual privacy review of state agency practices. The results help OPDP measure privacy maturity across 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.

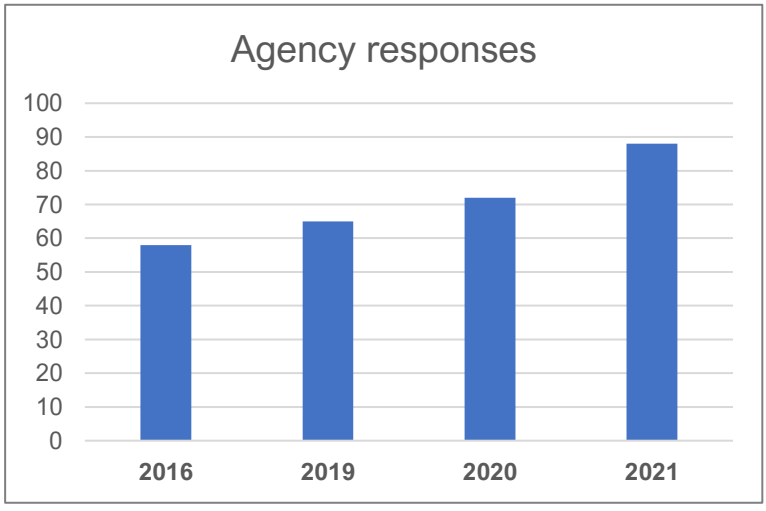
To help all agencies gain a common understanding of this year's assessment, OPDP hosted a webinar to walk through the survey and answer questions. Overall, this assessment covers many of the basic components of a privacy program and aligns with the Washington State Agency Privacy Principles.

Eighty-seven, out of 88 state agencies contacted[1], responded to the assessment this year – the highest response rate since its introduction in 2016. This year's 98.8% response rate is up from 82% in 2020.

Privacy maturity continues to build across the enterprise, but continued work is needed to ensure Washington residents' data and privacy is protected and personal information is handled appropriately.

Participation and Methodology

The State Chief Information Officer sent the assessment to agencies as part of the Office of the Chief Information Officer (OCIO) 2021 annual certification process. Each year agency partners are required to provide information to the OCIO to track compliance with statewide technology policies. Coupling the privacy assessment survey with the annual certification process makes it easier and more consistent for the OCIO and state agencies to collect and provide information.



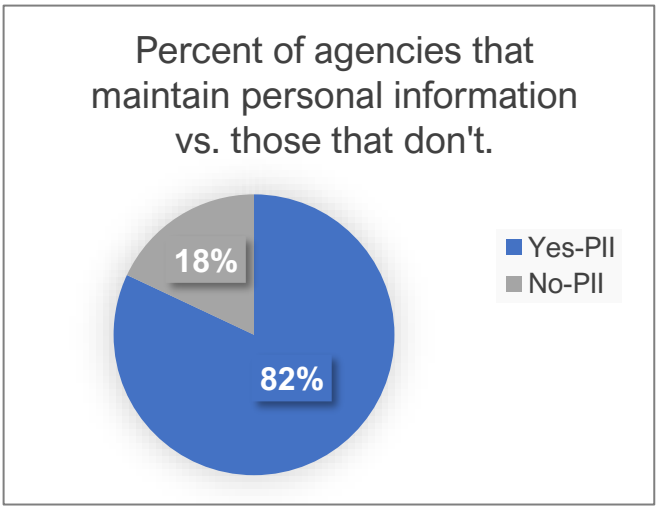
Of the 87 respondents, 72 agencies indicated that they collect and maintain some personal information. Data in this report is based on those 72 agencies.

[1] OCIO works with 88 state agencies as part of the annual certification process.

Personal information – also commonly referred to as personal data or personally identifiable information (PII) – is defined as information identifiable to a specific individual.

The 2021 Privacy Assessment Survey gathered information in several areas including:

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



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

Nearly 86 percent of agencies reported the importance of strong privacy protections has increased, up from two-thirds of state agencies in 2020. No agencies said privacy became less important. This reflects more awareness of privacy policies nationally, state action on new privacy laws, and general media coverage of privacy protections in the private sector.

Overall, OPDP found that agencies are more likely to have core privacy program components – such as dedicated staff and 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. This need will no doubt continue with the growth of privacy law and privacy protection requirements.

As a foundation for privacy program development, OPDP articulated the Washington State Agency Privacy Principles with the help of state agencies. These principles were finalized in October 2020 and this report makes those connections throughout.

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.

PRIVACY PRINCIPLES	
LAWFUL, FAIR, AND RESPONSIBLE USE	Collection, use, and disclosure is: • Based on legal authority. • Not deceptive. • Not discriminatory or harmful. • 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

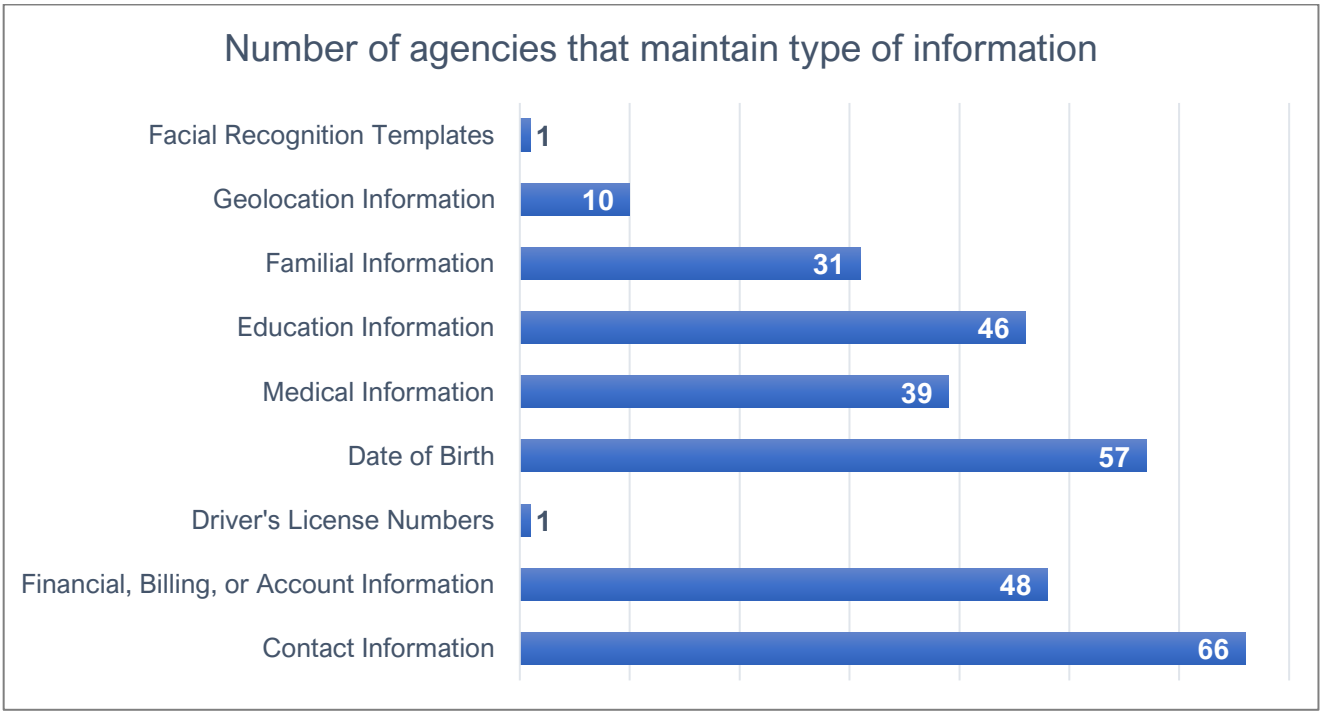
The privacy assessment gathered information from agencies about the types of personal information they maintain and the sources for that information. The assessment again revealed that many agencies maintain various types of sensitive personal information.

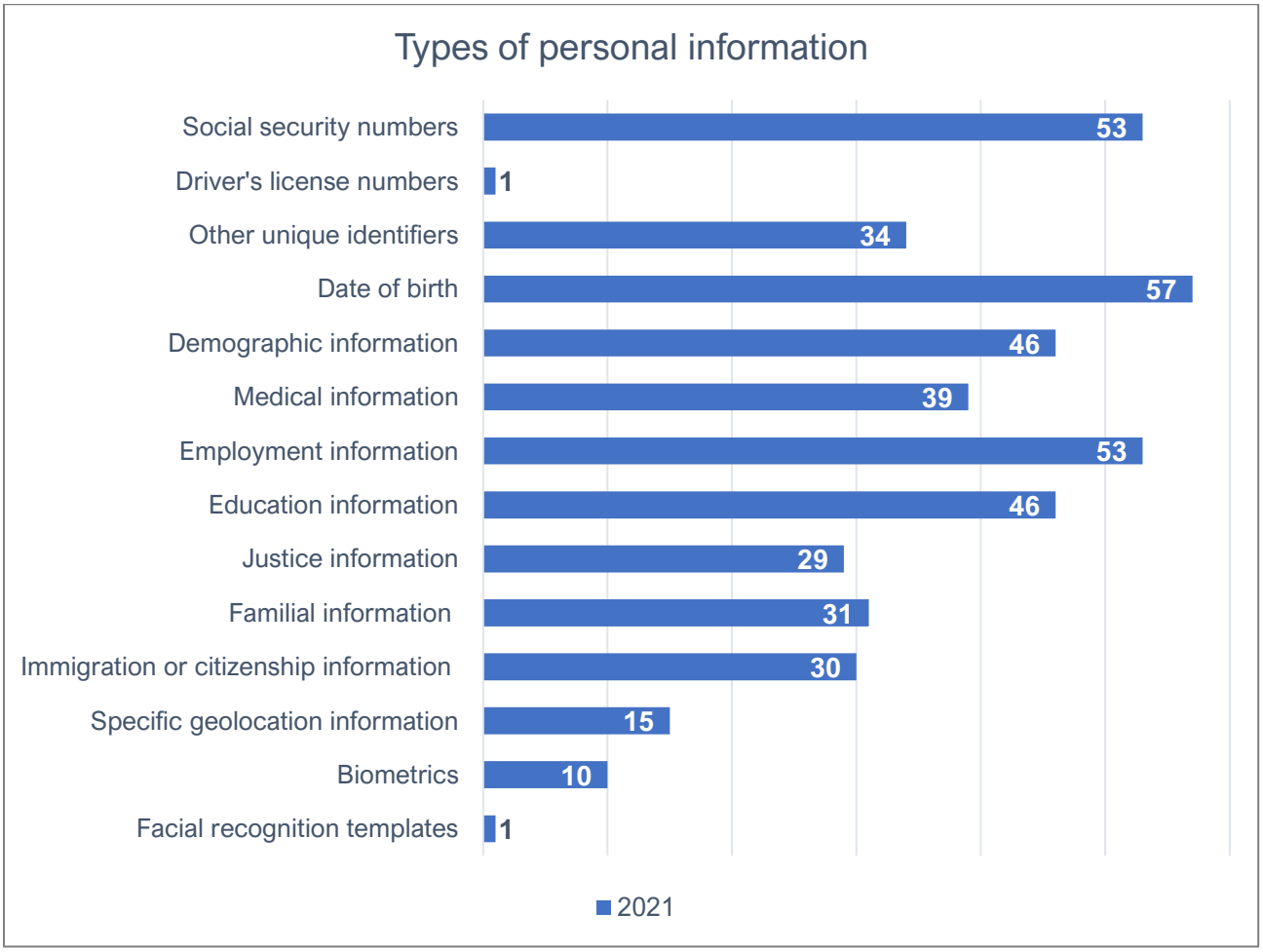
A broad range of data fits within the concept of personal information. It includes everything from basic contact information to social security numbers, detailed health information, immigration status and facial recognition templates. Different levels of protection are warranted for different types of 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 types of information the various agencies maintain varies widely, with a few agencies holding only contact information and many others maintaining far more sensitive information.

This bar chart shows how many agencies hold different kinds of data. The most common type of data held by agencies (66 agencies) is contact information.





Privacy Roles and 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.

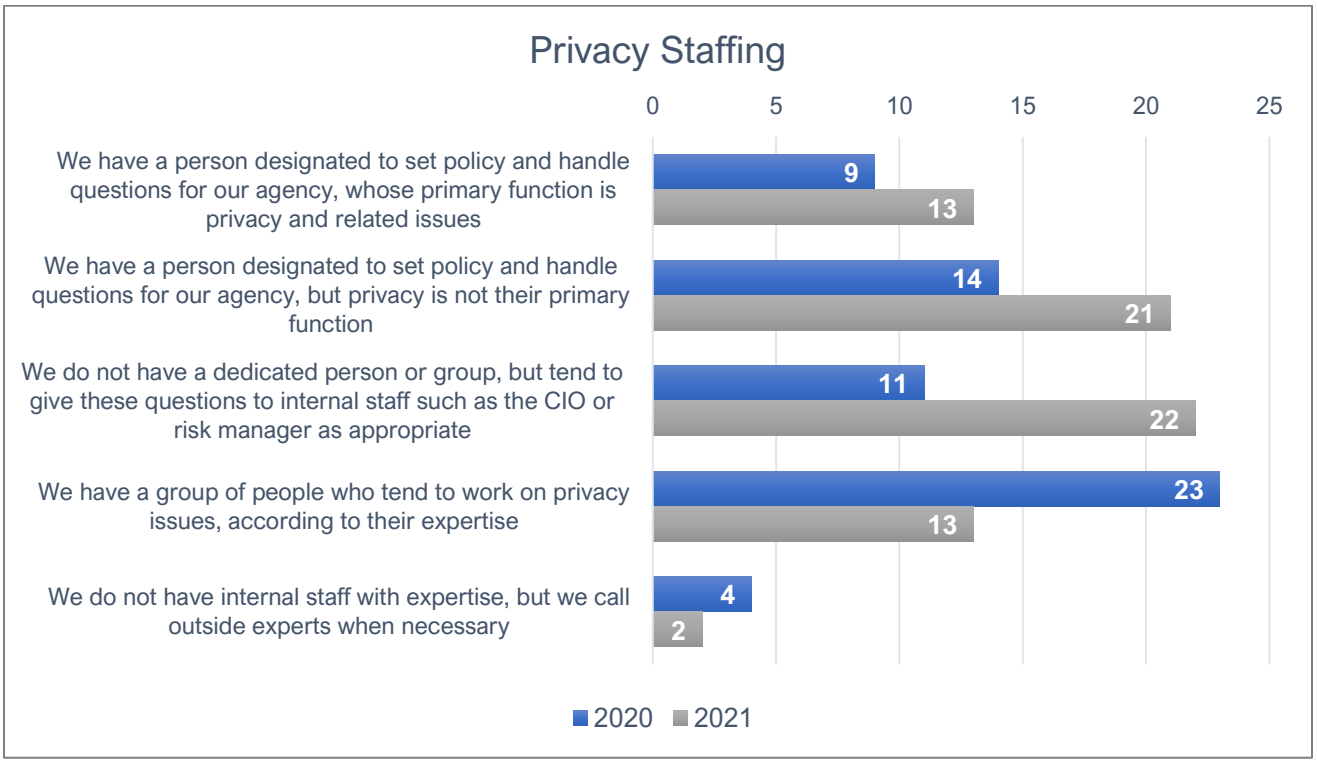
OPDP asked agencies to choose one of five potential staffing strategies that best described their approach to privacy. The options ranged from having a designated person whose primary job is privacy, to contacting external resources such as the Office of the Attorney General on an ad hoc basis.

For 2021, thirty-four agencies reported having a specific person designated to handle privacy policy and related questions, up from 23 in 2020. Overall, fewer agencies are reporting that no one does privacy policy, and more agencies across the board report a process for handling data privacy policy questions or inquiries.

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. Some agencies include privacy duties with cybersecurity or public records functions, both of which have some overlapping skillsets. However, privacy, public records, and cybersecurity are unique and different disciplines requiring distinct training and tasks.

OPDP is fostering a community of practice for privacy professionals at the state level to leverage the knowledge of active privacy professionals across the enterprise. Modeled on other existing communities of practice drawn across agencies, this group should develop into a resource for efficiently answering questions, attacking challenges, and offering insight into new initiatives.

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.



Above is data from the Office of Privacy and Data Protection 2020 results compared directly above the 2021 results.

Agency Training

Privacy policies and staff training are both foundational controls.

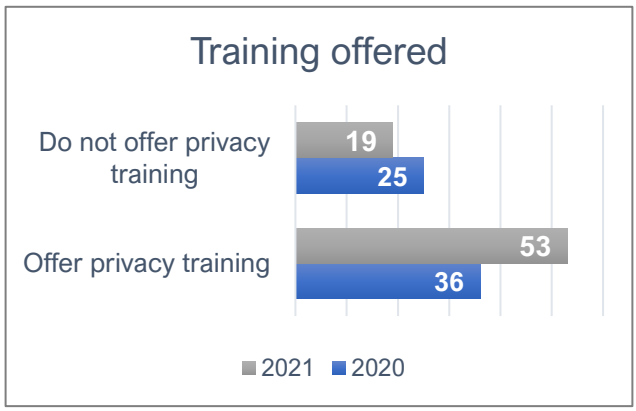
Internal policies apply to how information is collected, used and shared. They demonstrate that an agency understands the protections that apply to its information and has implemented appropriate standards. They are also one way to document the agency's commitments to how it will handle personal information.

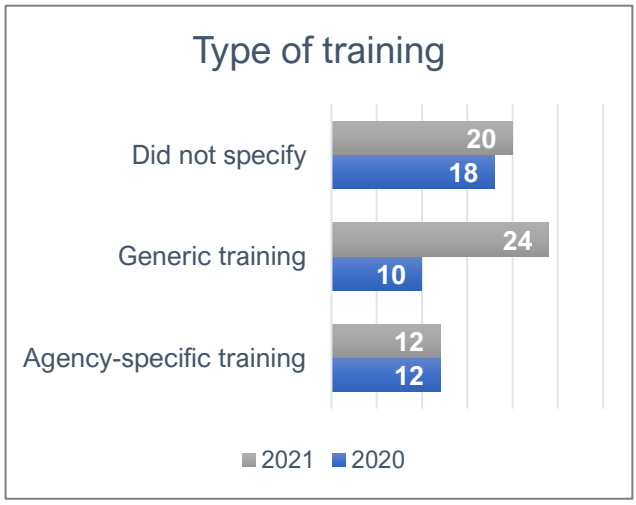
Training helps to ensure staff understand the importance of protecting personal information and how to do it. Without training, staff may not understand the commitments the agency has made. This is particularly important when dealing with privacy because many agency employees have access to personal 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.

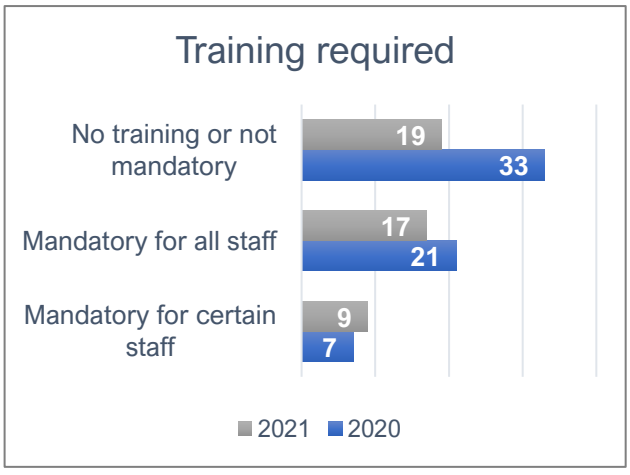
The OPDP is developing statewide training to help agencies build awareness of the importance of privacy. This basic privacy training is slated for release before summer 2022.

Agencies were asked the following questions about training:

- 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?







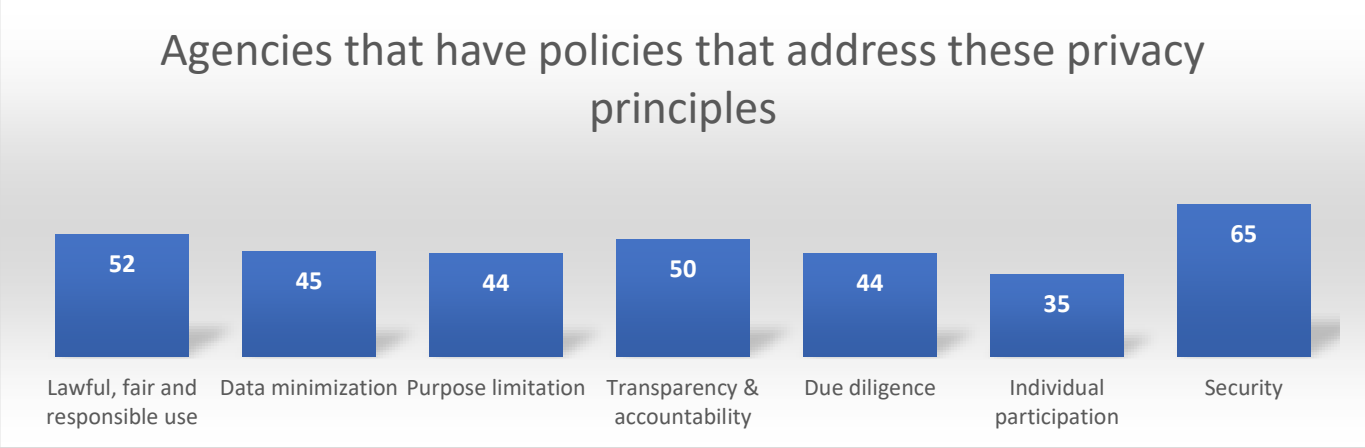
Although most agencies have privacy policies, fewer offer training to staff. Approximately 74% of the agencies with Washington resident's personal information indicated they offer some type of privacy training. This is up from 59% in 2020. The number of agencies that do not offer training has declined since last year.

Of the 53 agencies that offer training, about one-third reported generic privacy training, and 23% reported agency specific training. Approximately 28% 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 the agency has implemented.

There is a slight difference between training that is offered, and training that is required. Seventeen agencies reported that privacy training is mandatory for all staff, and another nine reported that it is mandatory for certain staff. Fewer agencies responded to this question in 2021.

Agency Privacy Policies

Another set of data that is important to note from this year's survey is the beginning of adoption of the Washington State Agency Privacy Principles developed by the Office of Privacy and Data Protection. Most state agencies that maintain personal data have started the process of adopting the concepts in the principles. It should be noted that adoption is inconsistent across the whole of state government. Some agencies have adopted but not fully implemented the state privacy principles, while others have adopted some but not all the state privacy principles. OPDP will continue to work with state agencies to adopt the privacy principles as well as with local governments (outside the scope of this report). The inconsistency in adoption is illustrated by the table below showing different numbers of agencies adopting each principle.



Agencies were asked about different types of privacy policies:

- Does your agency have formal privacy policies?
- Does your agency have formal policies or less formal standards that apply to subsets of particularly sensitive information or populations?

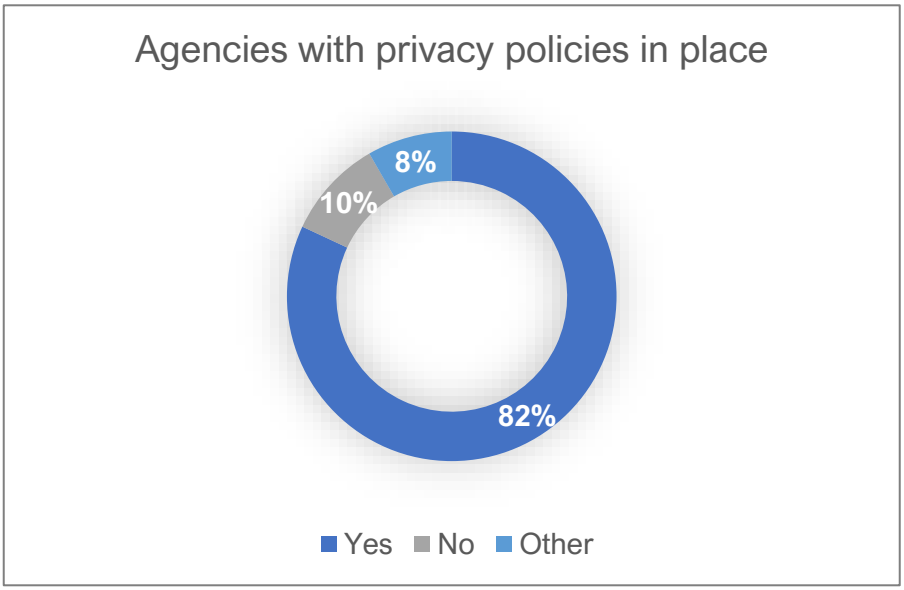
Most agencies have formal privacy policies and more agencies have implemented policies that include varying levels of protection for different information.

The increase of people working on privacy has resulted in more policy development. The result is 82% of agencies report having formal policies or procedures for privacy. This is up from 75% in 2020. The 59 agencies reporting a formal policy is up from the 45 in the 2020 survey.

Since last year's survey, many agencies have undertaken efforts to put in place new policies or improve the policies they had. This is reflected in fewer agencies reporting "other" to the question about formal privacy policies (see table below). Five agencies reported "other" in this year's survey, down from eight in the previous report. This most likely reflects more agencies with policy in process, and the completion of policies begun last year.

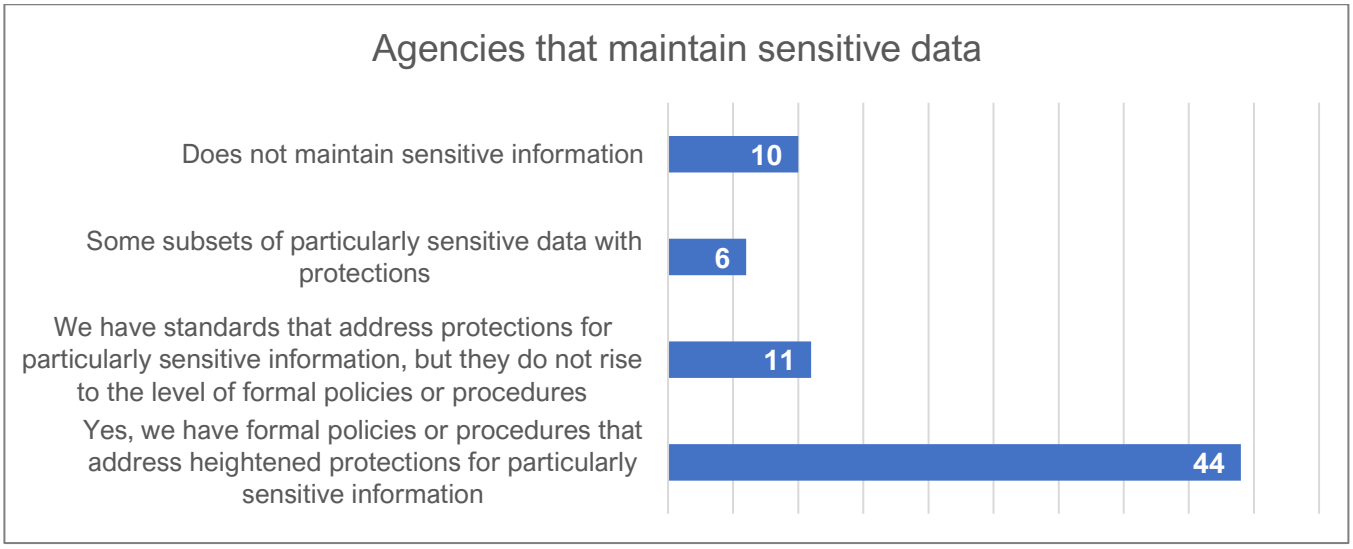
	Agencies with formal privacy policies		
Year	With policies	Without policies	Other*
2021	59	7	5
2020	45	8	8

**Several agencies indicated policies are in development.*

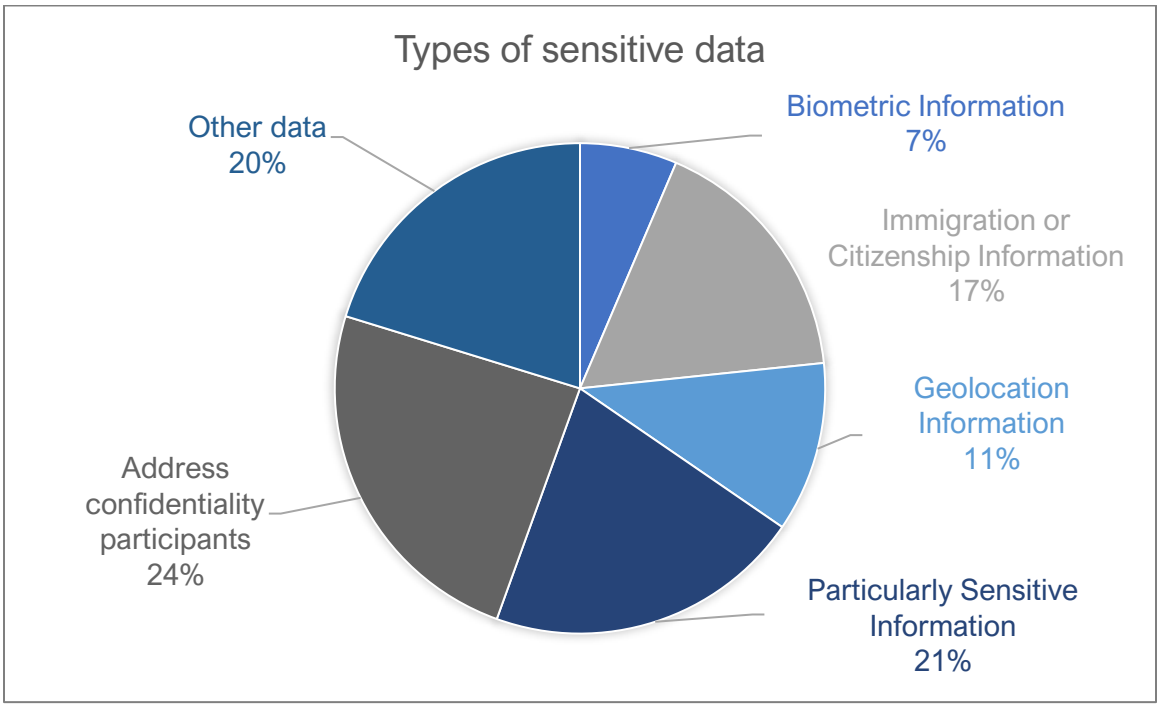


Since agencies maintain different categories of data, each category may require different protections and policies. For example, some agencies may have particularly sensitive data that requires more stringent protections and would have specific policies for that sensitive data, as well as more general privacy policies for all data maintained.

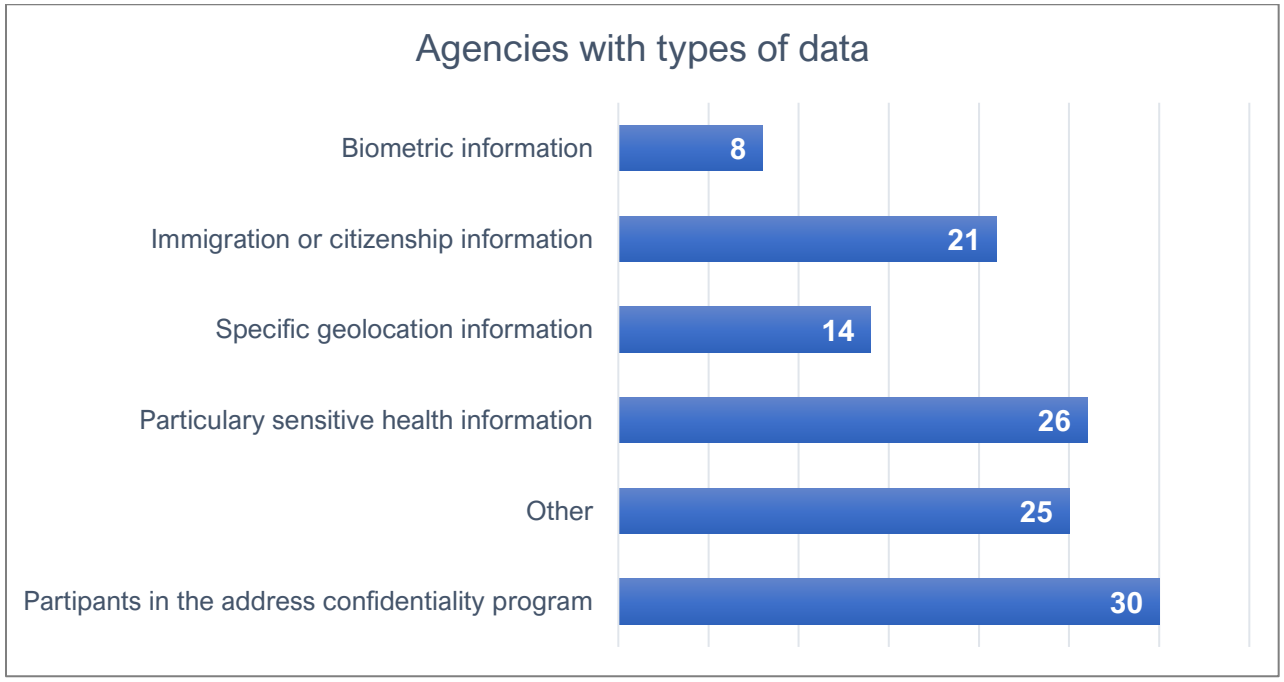
The table below shows agencies with formal policies or procedures, or other standards, that address heightened protections for particularly sensitive subsets of information.



This pie chart shows the kinds of data that is maintained and protected by policies, procedures or standards by percentages across the entire state government enterprise:



Here is the same data shown from the perspective of how many agencies maintain data in each of the same categories:



Transparency

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

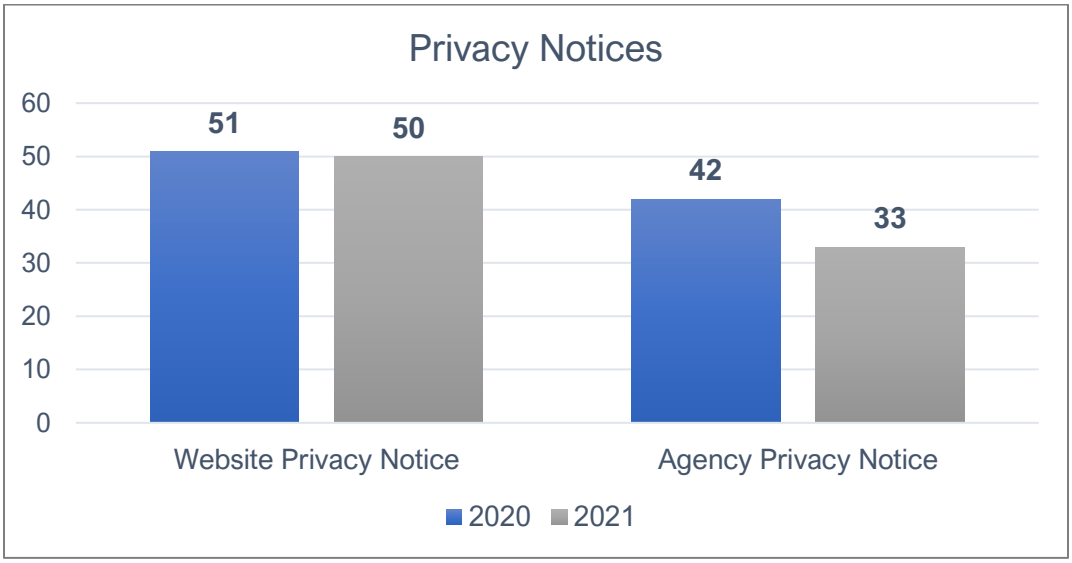
Agencies were asked about two types of commonly used external-facing privacy policies. Depending on context and preference, a privacy policy might also be called a privacy notice, notice of privacy practices, privacy statement, or simply privacy information.

Agencies were first asked about a website privacy policy, which addresses how information is gathered on the agency's website and how it is used. This type of policy addresses topics such as cookies and user tracking. Many agencies collect personal information in a variety of ways, including from online portals, paper forms, in-person, other agencies, or other third parties. This means a website privacy policy just covers one way agencies collect information about Washington residents. Fifty agencies indicated they have this type of policy.

Next, agencies were asked whether they have a more general privacy policy that contemplates 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.

More than half of the agencies with personal information (32), 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

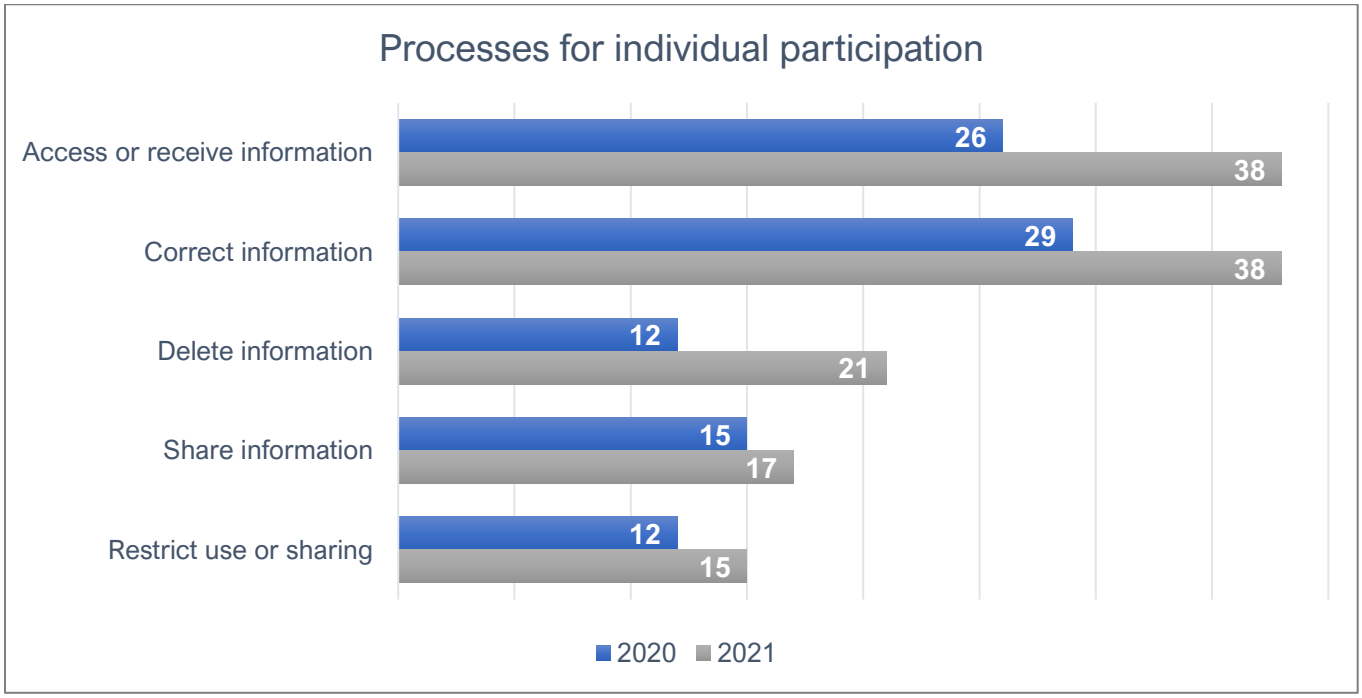
People should have control of their information whenever possible. This principle could be implemented by having processes for requests:

- 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 these activities would be appropriate for all agencies or all government functions. Overall, more than half of agencies indicated that they had at least one of these processes in place.

Agencies were asked if they had a process, policy, or procedure in place that would address a person's request to control their personal information. Forty-four agencies reported they have at least one, and 27 reported they do not have any procedures for individuals to control their personal data.

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.



Compared with 2020 data, more agencies give individuals control over their data in 2021.

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.

Agencies were asked about privacy incidents or breaches that occurred in the last year. Incidents and breaches are defined as:

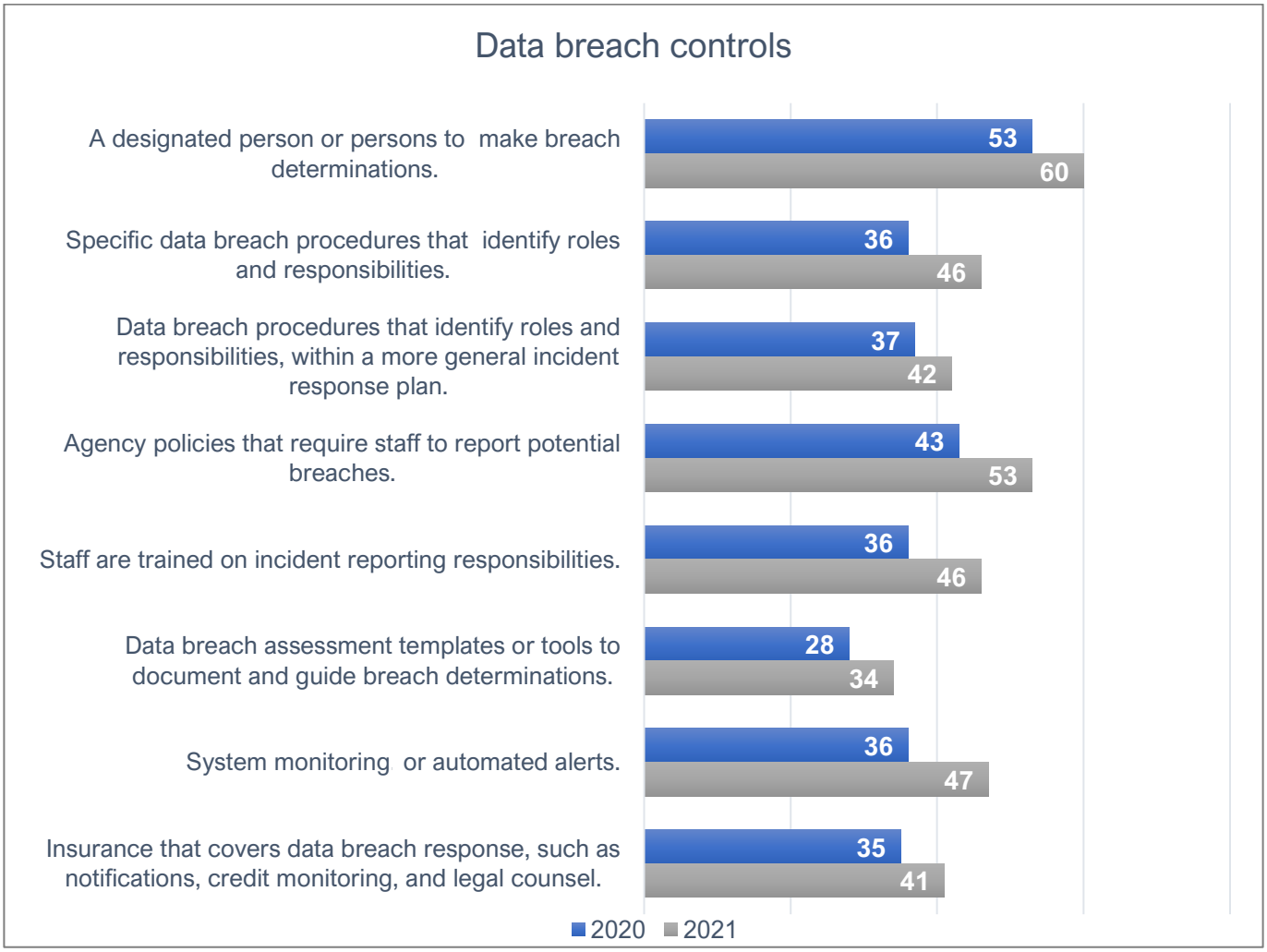
- An **incident** is the unauthorized use or disclosure of personal information, regardless of whether it requires notification under a breach notification law.
- A **breach** is an unauthorized use or disclosure that requires notification.

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 2020. Approximately the same number of state agencies reported one or more incidents and one or more breaches.

Detecting and responding to incidents 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 a state 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.

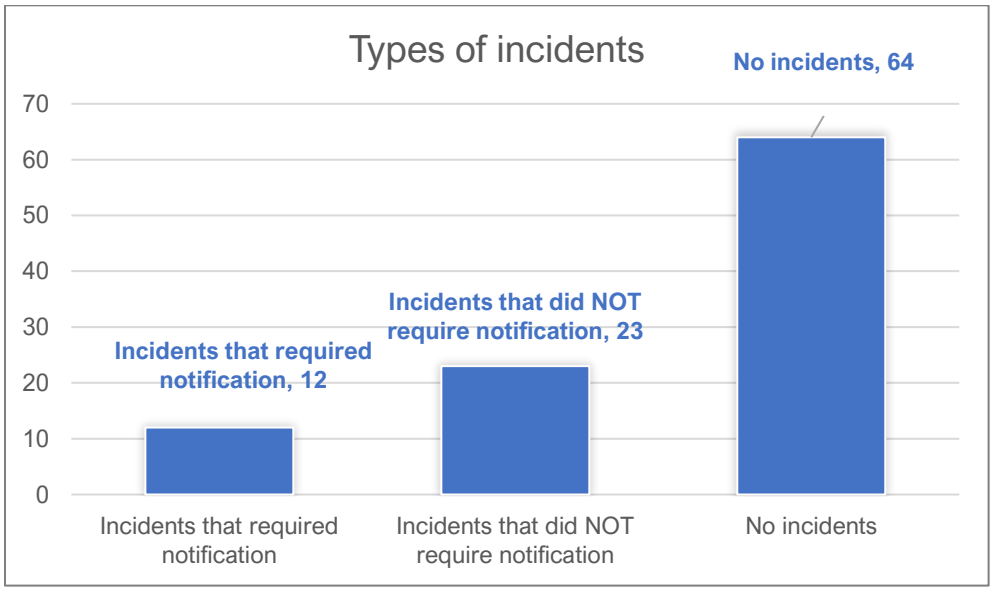
We asked agencies what steps they have taken to ensure incidents are discovered. Sixty agencies, up from 53 agencies last year, have designated at least one person to make breach determinations. About half of those have also implemented assessment tools or templates. Overall agencies are improving in how they deal with data breaches and incidents.



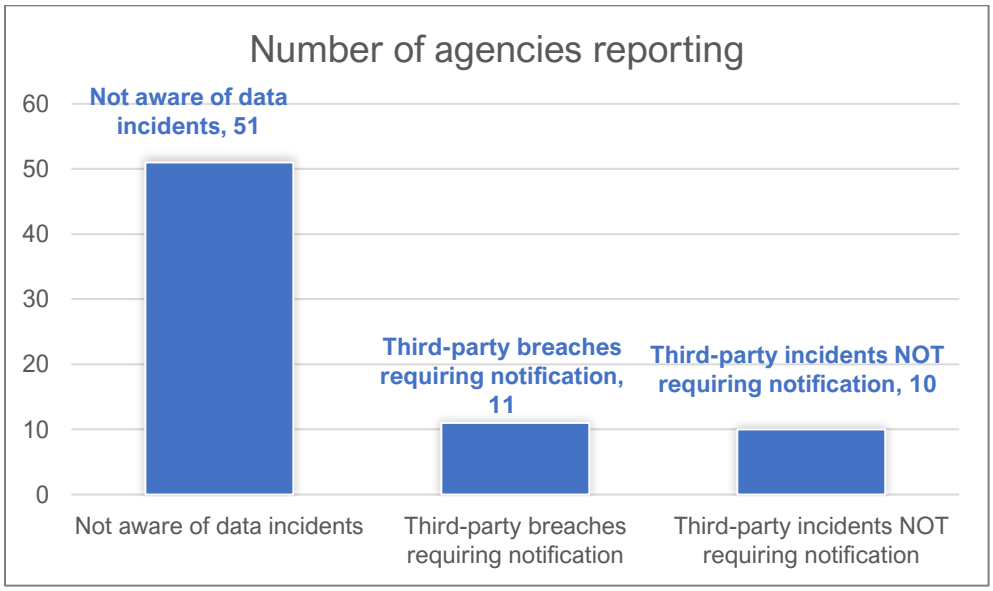
For the second year in a row, OPDP also asked agencies about incidents experienced by third parties they share information with. Third parties, such as service delivery providers, technology vendors and researchers, have significant access to personal information. Just as agencies must appropriately 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 agreements are also required though OCIO policy and RCW, including when sharing with third party vendors.

Below is data from the 2021 survey regarding agency data breach incidents and third-party incidents. The bar chart represents the types of incidents across the whole of state government, while the next bar chart shows the number of agencies experiencing the specific type of incident.

Agencies reported about 12% of incidents (nine agencies) that required breach notifications; 23% (12 agencies) had incidents that did not require notification; 64% (47 agencies) reported they are not aware of any data incidents over the past year.



In 2021, 51 agencies were not aware of any third-party breaches, 10 knew of data breaches which did not require notification, and 11 breaches were known to require notification.

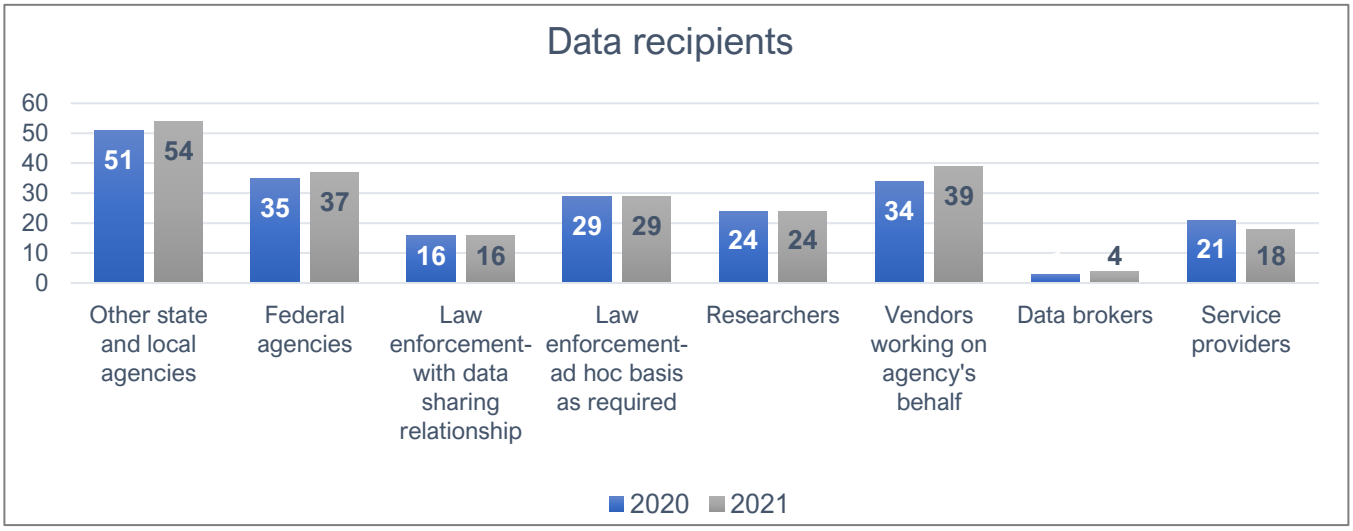


Data Sharing, Third Party Management, and Data Publishing

More than 75% of agencies share personal information with other state or local agencies.

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 survey also asked if agencies sold data, which is different from simply sharing data through a formalized agreement. In this report the term "sharing" is used broadly to cover many different types of data exchanges. Over 97% of state agencies do not sell personal information.

The chart below shows where information from agencies goes through sharing agreements or sale. Notably, almost all agencies share information with other agencies.



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. View the Data Sharing Implementation Guidance for more information.

According to the assessment:

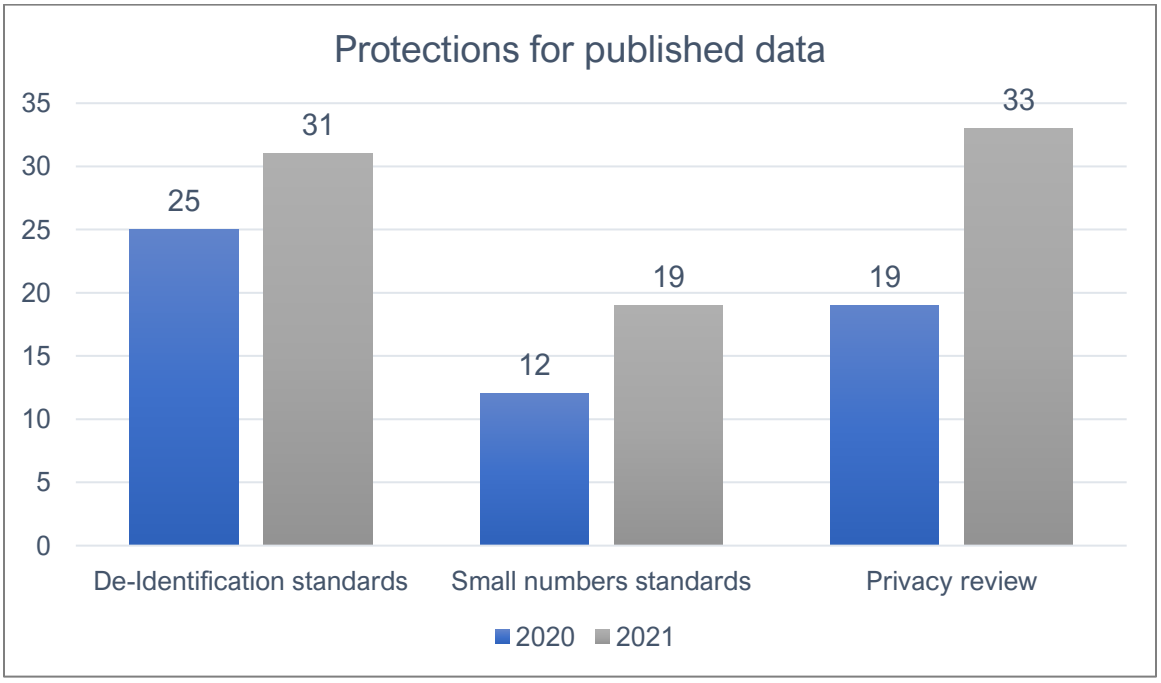
- 46 agencies reported they have a review process to ensure contracting, privacy and security are considered before establishing a new data sharing relationship.
- 39 agencies have designated specific people to approve data sharing.
- Eight agencies have established a committee to review data share requests.

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. Agencies can reduce the likelihood of published information being used to identify individuals by taking steps which include:

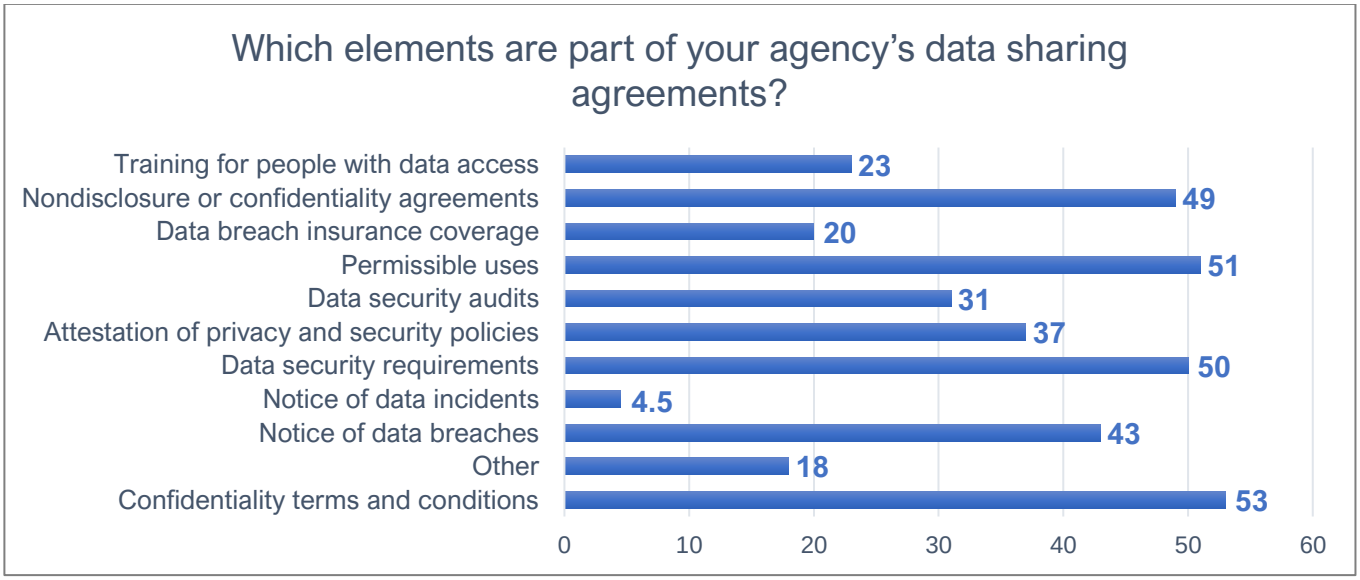
- Creating de-identification standards. De-identifying data requires removing more identifiers than just names. Having established standards for de-identification helps ensure appropriate and consistent practices.
- Following a small numbers standard. People can sometimes be re-identified when agencies 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 lower than 10 should not be published to avoid the risk of identification.
- 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.

Several agencies reported having these types of practices in place at their agencies for publishing public data.



State agencies are now required by OCIO policy and law (RCW 39.26.340 and RCW 39.34.240) to enter into data sharing agreements. Best practices and recommendations beyond these basic measures are part of a separate report created by the Office of Cybersecurity, Office of Privacy and Data Protection and the Attorney General's Office. State agencies should continue to improve their practices to protect and maintain data in their care.

New requirements were passed into law during the 2021 legislative session that require by statute data sharing agreements that had once only been required by OCIO policy. The new law has pushed many agencies to look for standardized agreements, and best practices for data sharing agreements. This chart shows the variance between agencies in what content was in agency data sharing agreements.

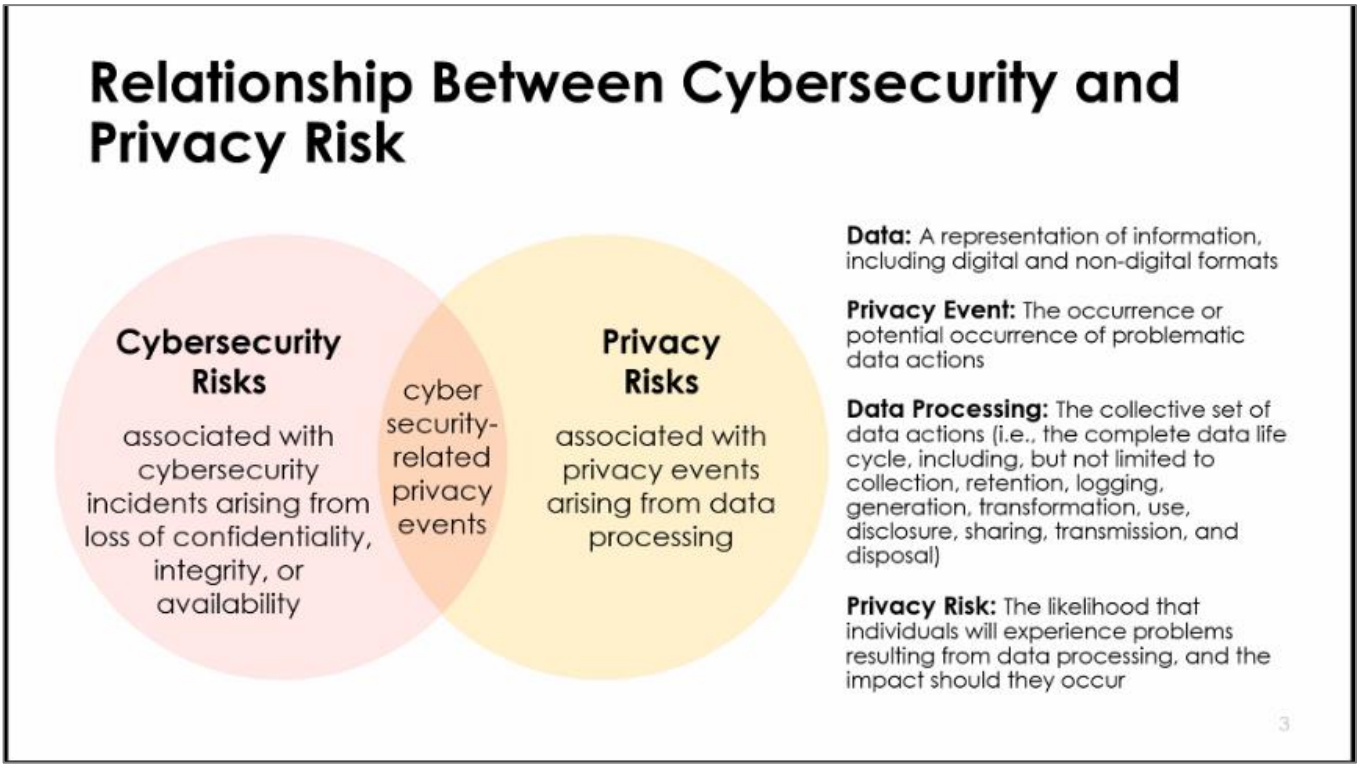


Moving forward (and with reference to best practices) agencies should continue to improve data sharing agreements and requirements around insurance coverage, training vendors, data use audits, and notification of data breaches. The passage of new requirements, and work by OPDP, the Office of Cybersecurity, and the AGO help to develop standards and best practices as noted in the 2021 Cybersecurity, Privacy and Data Sharing Agreements Best Practices report.

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.

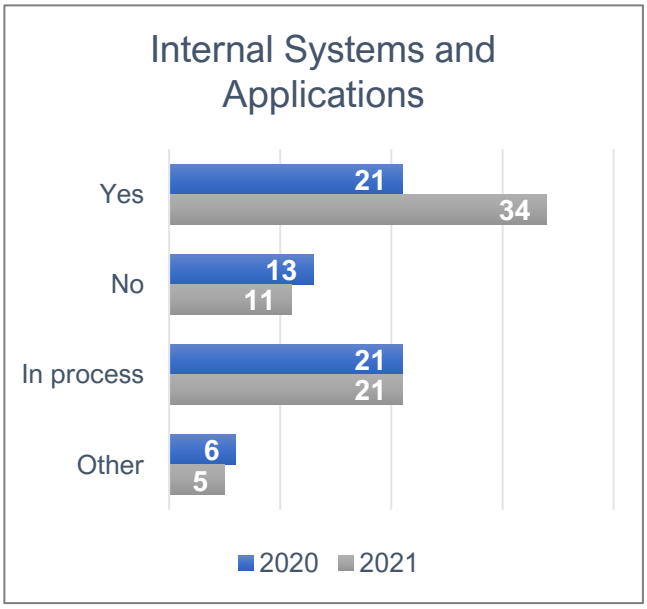
This data management step is very important in other ways as well. Data mapping and inventories are central to the overlap between the privacy and the cybersecurity disciplines. This inventory and process for data management becomes the keystone between the two frameworks, or the starting point for engaging organizations in the importance of both frameworks. The National Institute for Standards and Technology (NIST) Venn diagram also demonstrates the relationship between cybersecurity and privacy for data related events due to data processing activities.

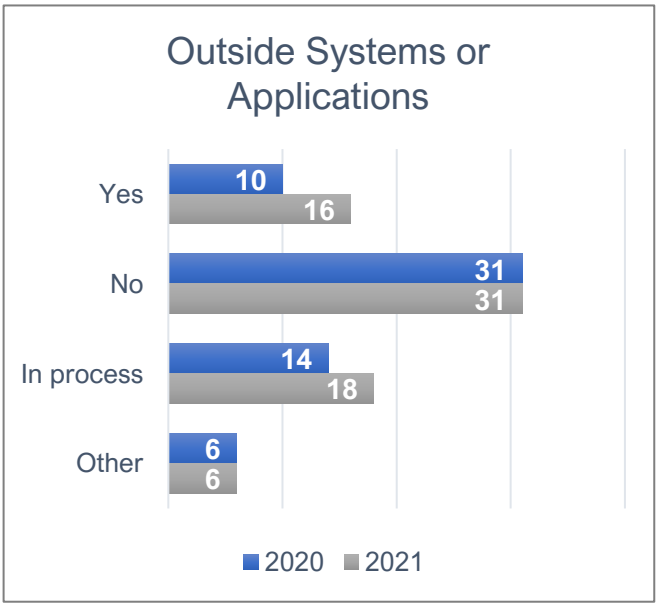


We asked agencies if they had completed a data map or inventory of systems and applications that includes the type of personal information maintained. We also asked whether agencies have completed a data map or inventory that includes information stored outside of systems and applications. The question 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.

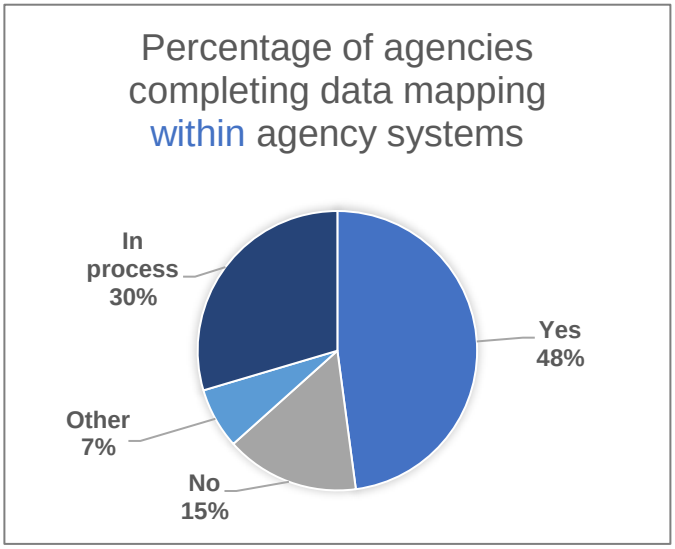
- In 2020, twenty-one agencies indicated they had completed a data map or inventory of personal information in systems and applications. This year, that number has increased to 34 agencies. This represents the fact that almost half of state agencies have done this inventory or map.
- Another 21 agencies indicated they were in the process of completing one. This is the same number as reported last year.
- In 2020, only 10 agencies had completed a data map or inventory that includes information stored outside systems or applications. That number increased to 16 this year, with an

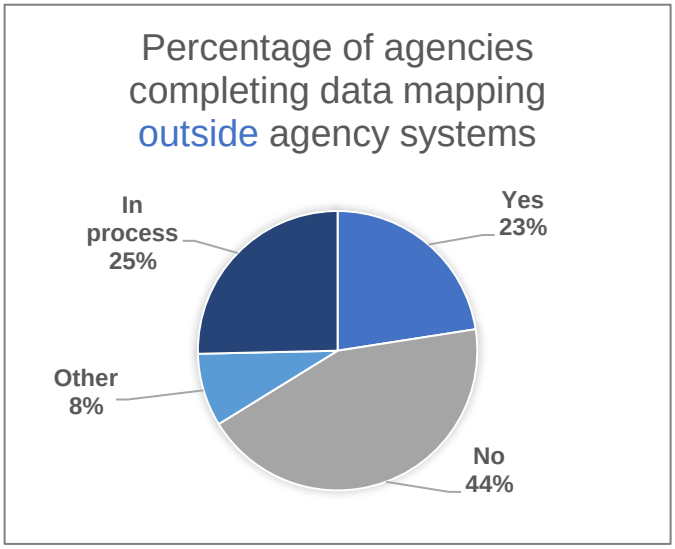
increase of two more agencies over last year in those agencies reporting mapping or inventories in process.





Below is the data from the 2021 survey which takes the raw numbers of agencies (shown above: 2021 - 34 agencies have an internal data map, 11 do not; 2021 - 12 agencies have a data mapping complete for data outside of agency systems, 31 do not) and where they are within the process of mapping data locations.





Regarding data *within* agency systems - 47% of the state agencies have completed data mapping; Almost 30% of agencies are in the process of completing a data mapping or data inventory process; 15% have not completed data mapping or data inventories.

These numbers change when agencies were asked about data mapping of data or information stored outside of agency systems. Only 23% of state agencies have completed this type of data mapping. Twenty-five percent are currently in the process of data mapping and inventorying; and 44% have not mapped or inventoried data held outside agency systems. As an inventory is both good data privacy policy, and good cybersecurity policy there is room for improvement on data inventorying and mapping.

The process of data management and data inventorying offers organizations an opportunity to implement data minimization strategies and delete unneeded data. This process can also lead to cost savings and reduces risk and liability (less data means less cost to store and protect data). In asking agencies about their data inventory practices, the 2021 survey also asked about agency practices regarding data deletion as part of data minimization strategies.

A number of agencies have data deletion processes in place. It should be noted that agencies that rarely delete old data may be required by statute to hold old data. Across state government:

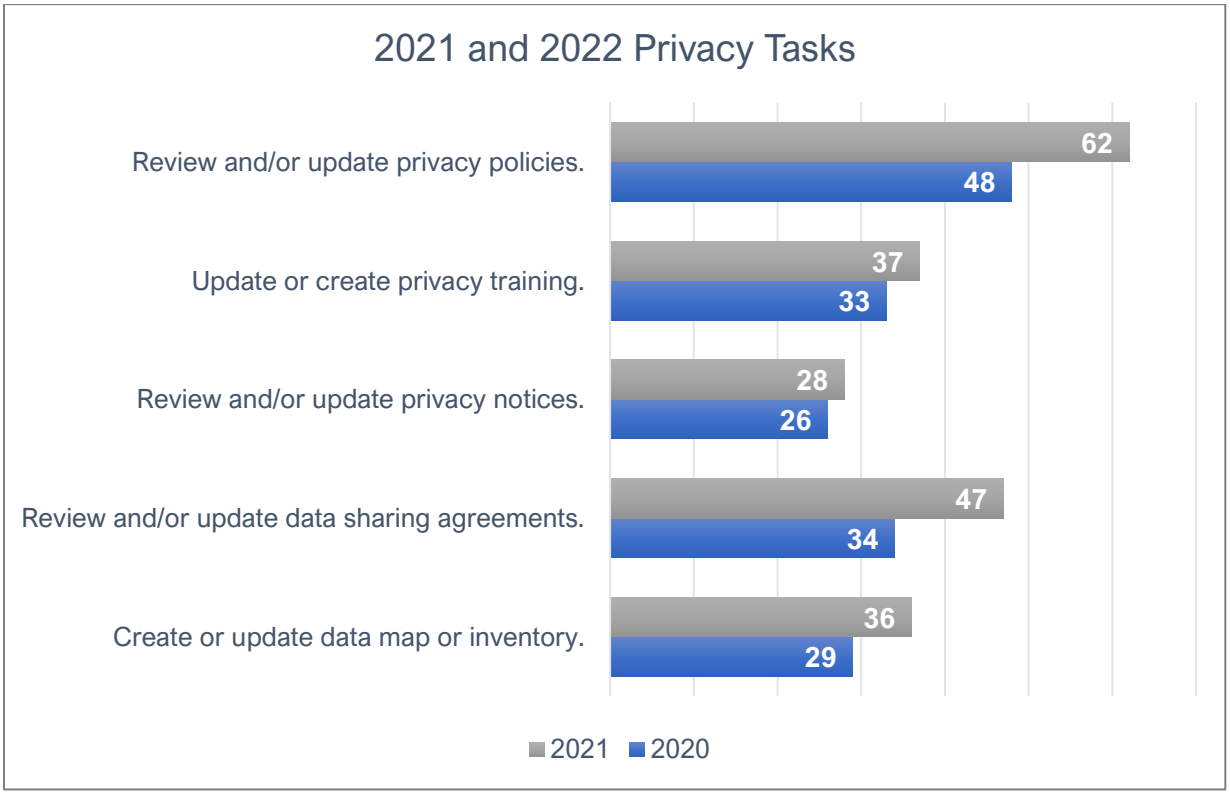
- 8% of agencies (12 agencies) rarely delete old data.
- 19% (28 agencies) of agencies have their records officer delete data.
- 28% (40 agencies) use automated tools to delete data.
- 44% of agencies (64 agencies) have individual work groups or programs responsible for deletion.

Note: agencies could choose more than one method, and so totals add up to more than 72 respondents.

Future Planning

Agencies were asked what privacy activities they already have planned over 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. The priorities of agencies stayed consistent over the year, except for reviewing or updating data sharing agreements. While data sharing agreement requirements have been in place as OCIO policy for many years, the recent attention by the legislature and new law passed in 2021 have resulted in some renewed attention by many state agencies.

This chart illustrates data from a future looking question. The gray bars are expected 2022 activities and the blue bars are expected 2021 (from the 2020 survey) activities.



The Office of Privacy and Data Protection looks forward to continuing our work with state agencies to develop and enhance privacy programs and increase privacy maturity across the enterprise. Please visit our website for more information and resources that our office provides at www.watech.wa.gov/privacy.

Contact

For more information or questions about this report, please contact:

Katy Ruckle, State Chief Privacy Officer at privacy@ocio.wa.gov.