WaTech
Washington Technology Solutions

2022 State Agency Privacy Assessment

Office of Privacy and Data Protection

Table of contents

Introduction

State agencies show continued improvement in the implementation of privacy protections, privacy awareness and privacy maturity.

RCW 43.105.369 requires the State 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.

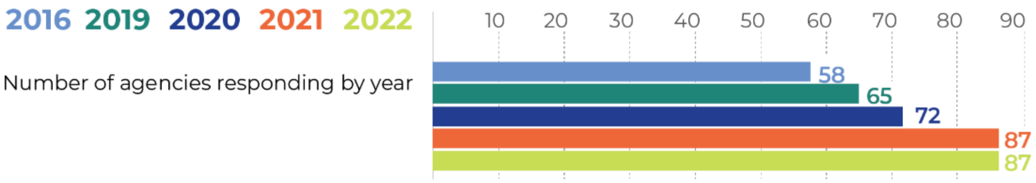
Agency roles and privacy requirements vary and best practices for one organization may not apply to another. This report is best viewed as a general assessment of privacy implementation across the state enterprise, and not an audit of specific agencies, or specific laws or policies.

Results from the 2022 survey indicate the state enterprise continues to improve in the implementation of privacy protections, awareness and maturity. This improvement is a result of increased awareness, cross agency collaboration, and the combined support from both the Governor and Legislature.

Overall, this assessment covers many of the basic components of a privacy program and aligns with the recently developed Washington State Privacy Framework, and the Washington State Agency Privacy Principles.

Nearly all state agencies surveyed (87 out of 88) responded to the assessment this year. This high level of response matches 2021 and is up from an 82% response rate in 2020.

Figure A



Privacy maturity continues to build and improve across the enterprise, but continued work is needed to ensure Washington residents' data and privacy are protected and personal information is handled appropriately. This is especially true as the privacy policy landscape continues to evolve.

Participation and Methodology

The State Chief Information Officer sent the privacy assessment survey to agencies as part of the 2022 annual technology certification process. Each year agency partners are required to provide information to track compliance with statewide technology policies.

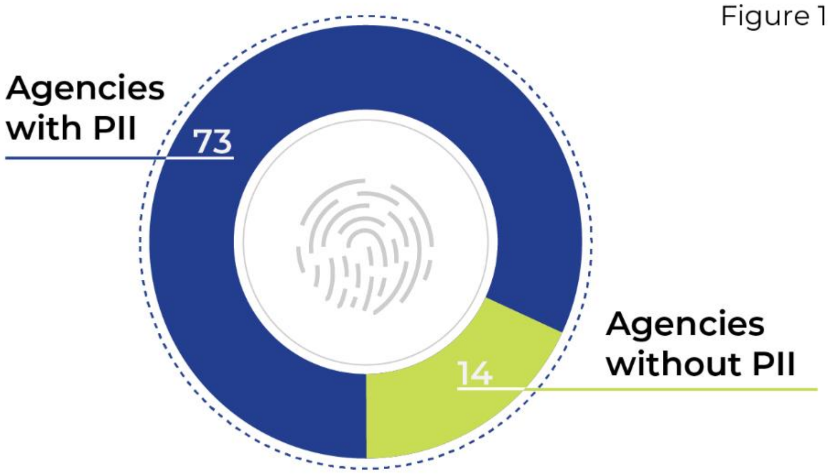
Coupling the privacy assessment survey with the annual certification process makes it easier and more consistent for WaTech and state agencies to collect and provide information. Of the 87 respondents, 73 agencies indicated they collect and maintain some personal information. Data in this report is based on 73 agencies. (In 2021, 72 of 87 agencies indicated they collect and maintain data).

Personal information – also commonly referred to as personal data or personally identifiable information (PII) – is defined as information identifiable to a specific individual. The 2022 Privacy Assessment Survey gathered information in several areas including:

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

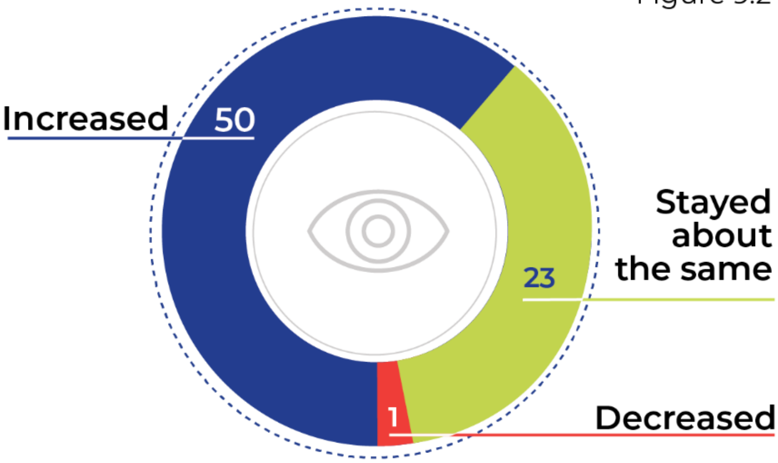
While the assessment helps gather valuable information about agency privacy practices, it is inherently quantitative. For example, it may measure whether an agency has formal policies and staff training but does not evaluate the adequacy of the policies or measure the effectiveness of the training. Data gathered for this report is an overall annual privacy review of the state as an enterprise.

Figure 1.0



Many agencies in 2022 again reported the importance of strong privacy practices. The trend towards the importance of privacy policies began to increase in 2021 with 86% of state agencies reporting strong privacy practices were important. In this year's survey for 2022, only one agency said privacy became less important. In 2022, 50 state agencies reported that privacy importance increased, while 23 agencies reported the importance had stayed about the same. The OPDP believes this reflects more awareness of privacy policies nationally, state action on new privacy laws, and general media coverage of privacy issues in the private sector.

Figure 9.2

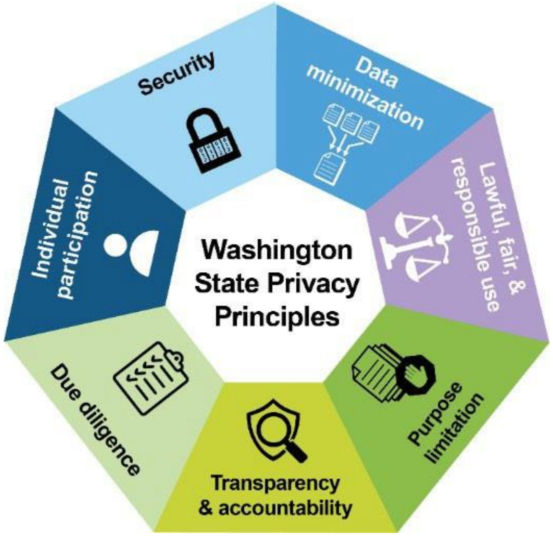


Overall, OPDP found that agencies are more likely to have core privacy program components – such as dedicated staff and formal policies and trainings than in the past. However, significant gaps remain and even agencies with more privacy experience consistently indicate they need additional resources. This need will no doubt continue with the growth of privacy laws 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 connections between the survey data and the principles throughout.

OPDP launched Washington specific privacy training in 2022 based on the Washington Privacy Principles and Washington state law.

OPDP also created a Washington State Privacy Framework based on state structures and the National Institute of Standards and Technology (NIST) privacy framework. The goal of this framework is to give state agencies and local jurisdictions easy access to a roadmap for measuring and improving privacy practices within their organizations.


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

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.

Washington State Privacy Framework

Privacy frameworks include the basic structure and concepts needed to build an effective privacy program. They include the components that should be included in a privacy program, but do not dictate how the goal of each component is achieved.

The Privacy Framework for State Agencies was developed based on the NIST Privacy Framework and other privacy program best practices. It is intended to be a flexible and scalable starting place for agencies of varying size to handle personal information of varying sensitivity. Agencies should use this framework to build out more agency-specific resources that form a privacy program skeleton to be expanded and adapted over time. Not all agencies will have all of the framework components in place but using this framework can help identify and prioritize risks and opportunities. This framework, introduced in 2022, can also be seen as a roadmap towards better privacy maturity for organizations.

Types of Personal Information

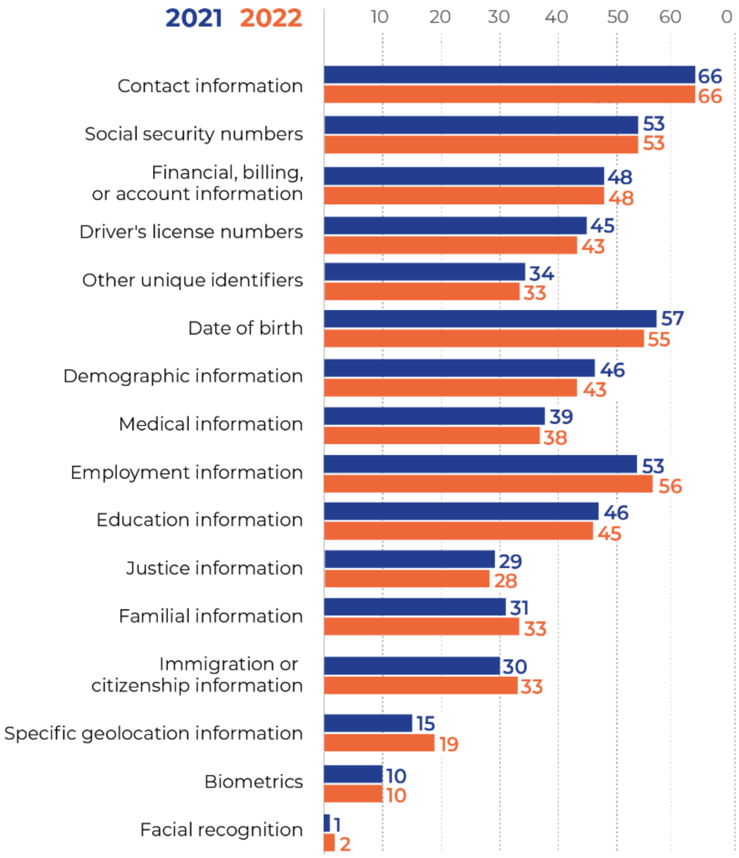
The privacy assessment gathered information from agencies about the types of personal information they maintain and the sources of that information. The assessment once again demonstrated that many agencies maintain various types of sensitive personal information.

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 needed for different types of information, depending on its sensitivity. State agencies hold or maintain data due to requirements in law, and to provide services.

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 that agencies maintain vary widely, with most agencies holding contact information and others maintaining far more sensitive information. This bar chart (Figure 1.1) shows how many agencies hold the most

Figure 1.1



common kinds of data. The most common type of data held by agencies (66 agencies) is contact information (a number unchanged from 2021 to 2022).

Privacy Roles and Staffing

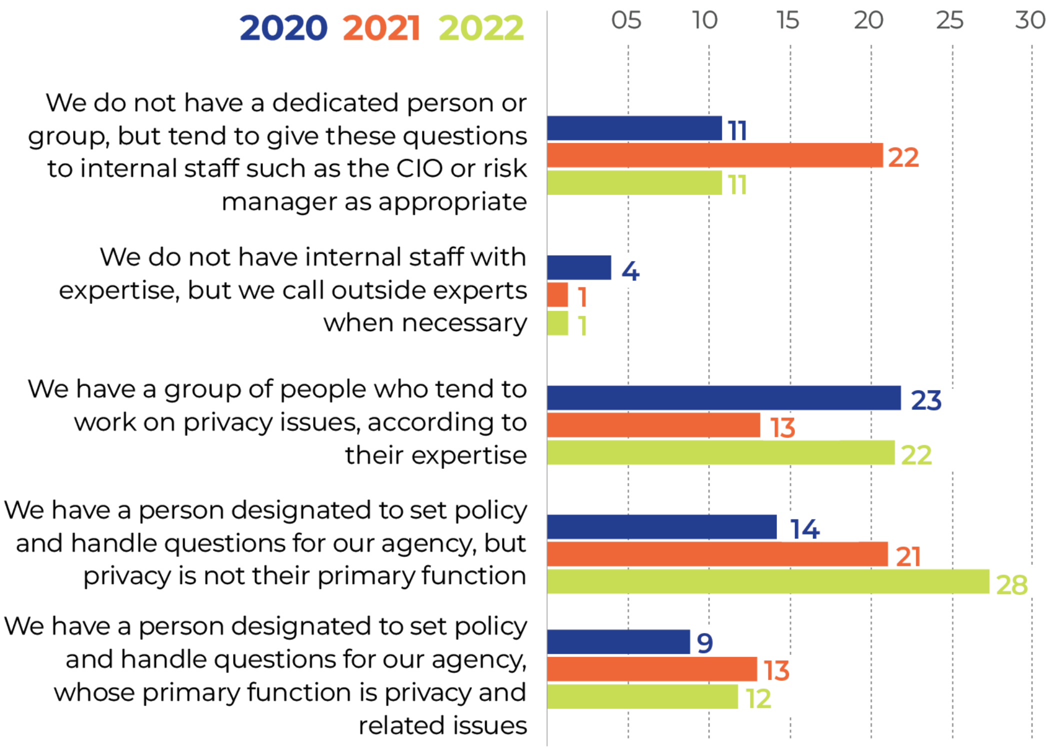
Agencies cannot adequately protect personal information without appropriate resources. The level of resources needed varies depending on the size of an agency, the functions it performs and the types and amount of personal information it maintains.

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.

In 2022, 40 agencies said they have a specific person designated to handle privacy policy issues (either as a primary or secondary responsibility).

Figure 2.1 compares 2020, 2021, and OPDP 2022 survey results for staffing.

Figure 2.1



This is an increase of six agencies since last year and continues the trend of more agencies having dedicated individuals responsible for these issues. For 2021, 34 agencies reported having a specific person designated to handle privacy policy and related questions, up from 23 in 2020. Another clear improvement for the enterprise is that fewer agencies are reporting that no one does privacy for the agency. The number of agencies that do not have a dedicated person or group dropped by half.

More agencies across the board also report a process for handling data privacy policy questions or inquiries. Only one agency, (down from four) reported that it depends on outside help for dealing with privacy concerns.

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.

Work that the OPDP is doing at an enterprise level demonstrates how agencies can commit personnel to a task, and central resources can then be leveraged to enhance the skills of that personnel no matter where they are within the enterprise.

For example, the 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.

Dedicated staffing also allows the OPDP to assist customer agencies with privacy work, training, or program development. The office also helps launch enterprise initiatives like the Privacy Basics Training for Washington State Employees and the state privacy framework.

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. Privacy policy implementation is a team effort in finding ways to both enhance innovation and protect data privacy of the people served by state government.

Agency Training

Staff training and privacy policies covered in the next section are both foundational controls that should be important pieces of any privacy program.

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 or the requirements the agency must follow for compliance. This is particularly important when dealing with privacy because many agency employees have access to personal information on a routine basis. Staff are the frontline when it comes to data protection. Taken together, strong training and clear policies are important pieces of the transparency and accountability privacy principle.

The OPDP developed statewide training to help agencies build awareness of the importance of privacy. This foundational privacy training was prioritized after past surveys indicated agencies were interested in standardized state offered training.

This Privacy Basics training for Washington State Employees is available to all state agencies through the enterprise learning center or via the OPDP website.

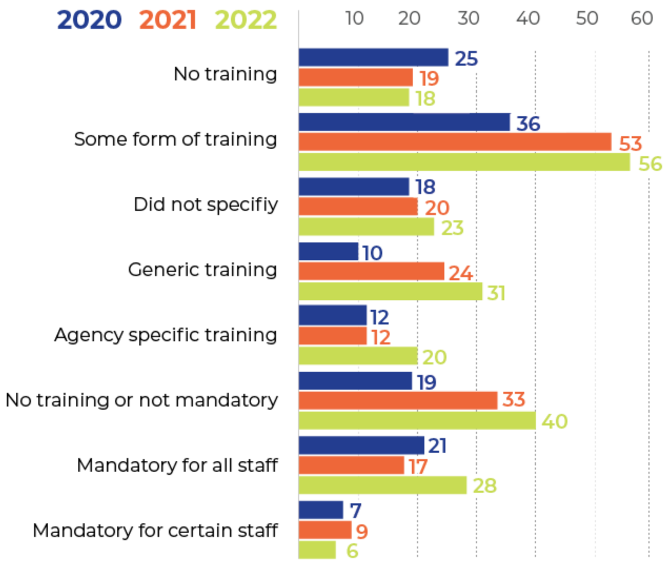
State agencies have incorporated this training into their mandatory training for employees. This training will help increase awareness and protection across the state enterprise. Washington state is one of only a few states nationally that has created state specific training focused on privacy policy and good data management.

The OPDP, for example, created a formal two-day workshop training to support agencies and individuals practicing and applying privacy principles. It is an excellent example of how OPDP as an enterprise-focused office can push out benefits and standards across dozens of state agencies in an efficient manner to support agency privacy professionals.

Agencies were asked the following questions about training (figure 3.5):

- 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?

Figure 3.5



The 2022 data shows more agencies offer privacy training than in the past. Often, privacy training is mentioned within, or is part of cybersecurity training. Standalone privacy training (either generic or specific) is beneficial for a better awareness of agency privacy policies. Approximately 75% of the agencies with Washington residents 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 any form of privacy training has declined from 25 in 2020 to 18 in 2022.

Of the 56 agencies that offer training, 31 agencies reported generic privacy training, and 20 reported agency specific training. (Twenty agencies 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 tailored to the types of information the agency maintains and the specific policies the agency has implemented.

There is a slight difference between the training that is offered and training that is required. Twenty-eight (up from 17) agencies reported that privacy training is mandatory for all staff, and another six (down from nine) reported that it is mandatory for certain staff.

This is an area the OPDP will continue to watch as the state-specific OPDP developed privacy training will continue to be utilized across the enterprise. The expectation is that more agencies will adopt the OPDP training, and this area will continue to improve. The OPDP prioritized creating a statewide privacy training program based on information from past surveys.

Agency Privacy Policies

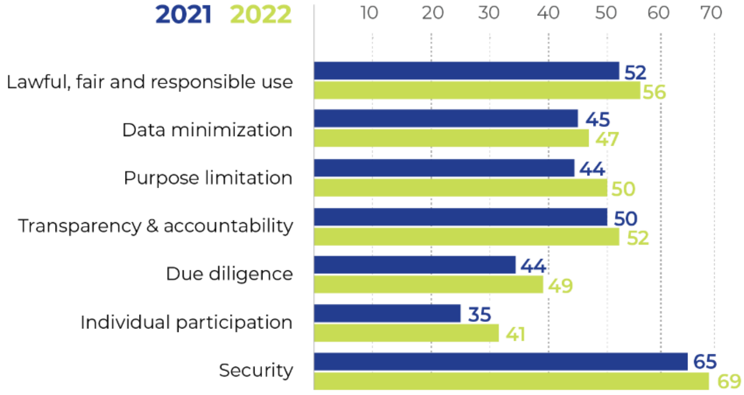
Internal agency privacy policies apply to how information is collected, used and shared. They demonstrate that an agency understands the protections that apply to its information and has implemented appropriate standards. Policies are also one way to document the agency's commitment to how it will handle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

Another set of data that is important to note from this year's survey is the continued adoption of the Washington State Agency Privacy Principles. Most state agencies that maintain personal data have started the process of integrating the concepts in the principles for agency data protection. 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 incorporated some but not all the state privacy principles. The OPDP will continue to work with state agencies (and local governments) to adopt privacy principles.

Of note in figure 3.6 is the trend of more agencies having more specific policies in place across all principles. The number of specific policies increased year over year from 2021 to 2022. This is another example of continued improvement across the state directly tied to OPDP work.

The number of state agencies that have policies that directly cover these privacy principles, year over year, are also indicated in figure 3.6.

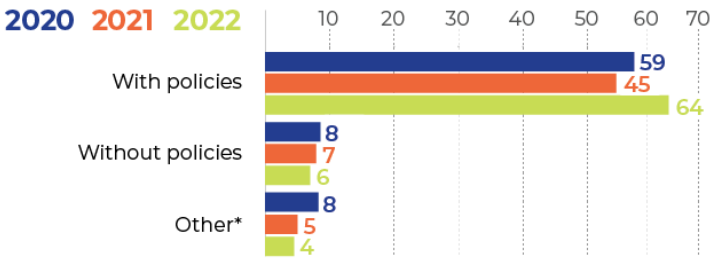
Figure 3.6



These numbers seem to be the result of two factors: 1) The increase of people working on privacy and 2) the greater awareness and importance of privacy. Both factors have resulted in more policy development. Support from legislative and executive branch leadership has also helped. The result is more than 87% of agencies report having formal policies or procedures for privacy. This is up from 75% in 2020. The 64 agencies reporting a formal policy is up from 45 in the 2021 survey.

Since last year's survey, many agencies continue to put in place new policies or improve the policies they have. This is reflected in fewer agencies reporting "other" to the question about formal privacy policies (see figure 3.7 for year-by-year comparisons). Four agencies reported "other" in this year's survey, down from eight in the 2020 report, and five in the 2021 report. This most likely reflects more agencies with policies in process, and the completion of policies begun in the past.

Figure 3.7

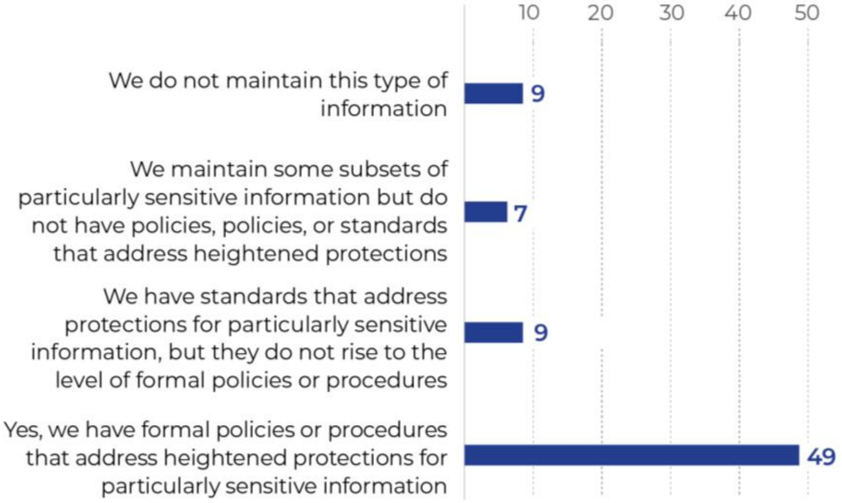


Since agencies maintain different categories of data, each category may require different protections and policies. For example, some agencies may have particularly sensitive data that requires more stringent protections and would have specific policies for that sensitive data, as well as more general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

Figure 3.2 shows agencies with formal policies or procedures, or other standards, that address heightened protections for particularly sensitive subsets of information.

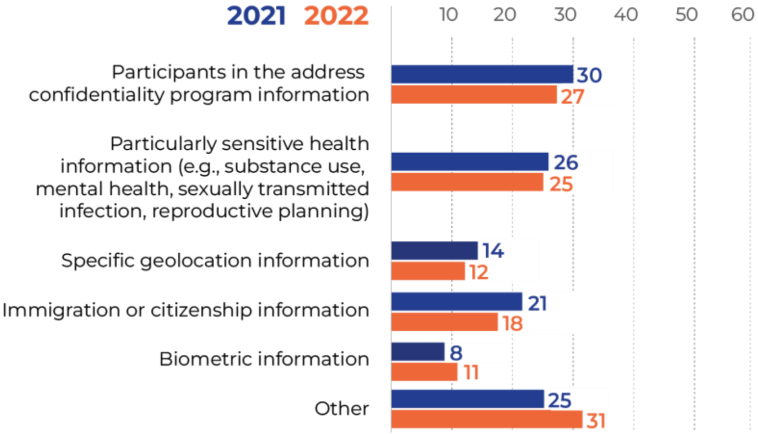
Agencies don't just need people in place to implement good privacy programs, agencies also need formal policies and procedures in place that address privacy. The survey asked how many agencies have those formal policies and procedures in place. Privacy policies should be focused on the specific types of information that need to be protected.

Figure 3.2



This survey drilled deeper into some of the exact kinds of data protected by policy. Via the survey questions we see the specific kinds of data protected by policies, procedures or standards at how many agencies (figure 3.4). The types of data requiring specific polices includes information from the state address confidentiality program, health information such as substance use, or mental health data, specific geolocation information, or immigration or citizenship information, as well as biometric information.

Figure 3.4



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 communicated clearly.

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.

In 2022, most agencies surveyed (64) indicated they have privacy policies in place (figure 4.1). Only six indicated they did not have privacy policies in place and four indicated that policies were in development.

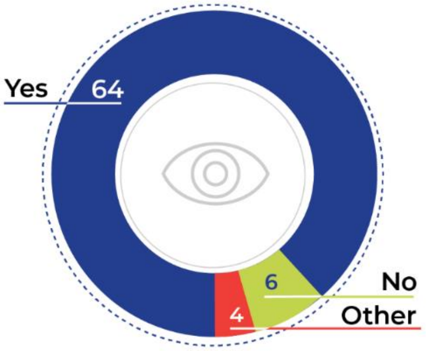
Agencies were asked about different types of privacy policies:

- 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?

Agencies were also 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. In 2022, 62 agencies indicated they have a website privacy policy.

Figure 4.1

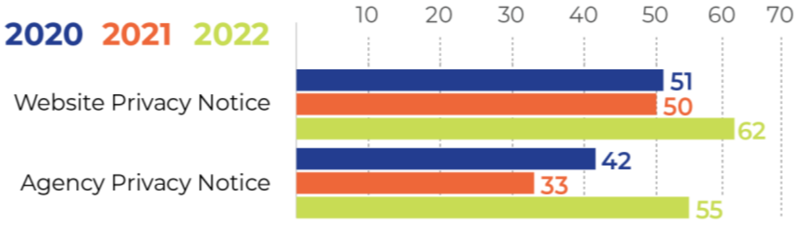


Agencies were also asked whether they have a more general privacy notice that contemplates the personal information the agency gathers from various sources. Typical information included in this type of notice would be at least:

- 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 (55), indicated they have this type of comprehensive privacy notice in 2022. Most agencies post it on their website, while some also mail the notice or provide it in-person. This could be an opportunity for improvement, as many of these privacy notices have not been updated in the past year. Only 19 agencies reported that they have updated their privacy notices within the last year, and eight reported it had been more than five years since they updated these notices (see Figure 4.2).

Figure 4.2



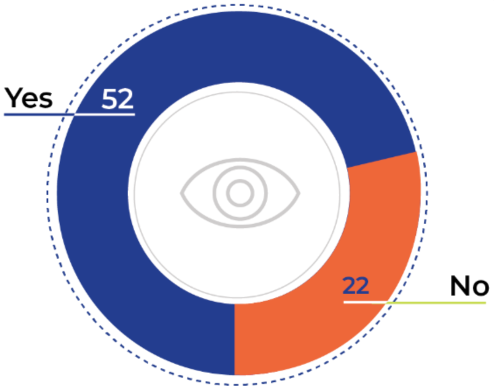
Individual Participation

People should have control of their information whenever possible. The Individual Participation 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 are appropriate for all agencies or all government functions.

Figure 5.1

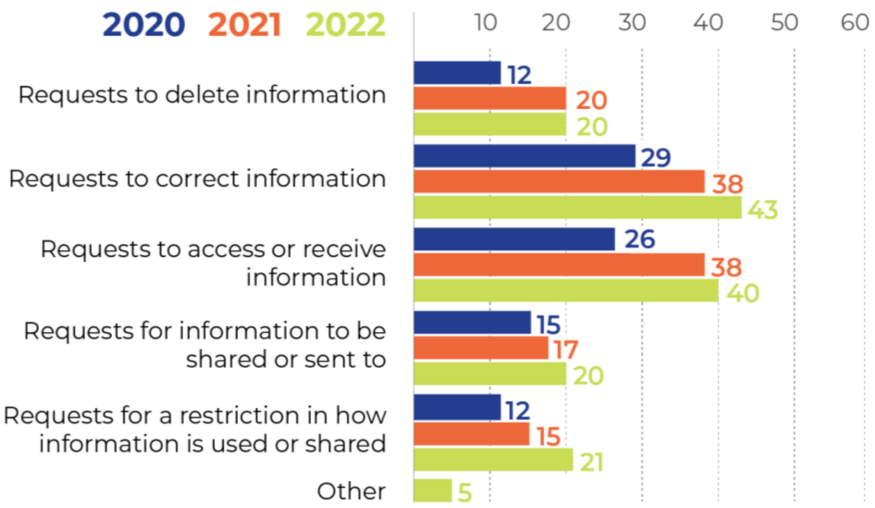


Overall, more than half of agencies indicated that they have at least one of these processes in place. Agencies were asked if they had a process, policy, or procedure in place that would address a person's request to control their personal information. Fifty-two (up from 44 in 2021) agencies reported they have at least one, and 22 (down from 27 in 2021) reported they do not have any procedures for individuals to control their personal data (see figure 5.1).

As shown in figure 5.1a, agencies more agencies had a process for people to correct inaccurate information. The next most common policy in place is a process for people to access or receive information, which makes sense considering agencies' obligations under the Public Records Act. These priorities are the same across the last three years of survey data.

OPDP will watch for changes in this metric as residents of Washington state may expect more involvement as new privacy laws in California, Virginia, Colorado and other states are implemented.

5.1.a



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.

- 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.

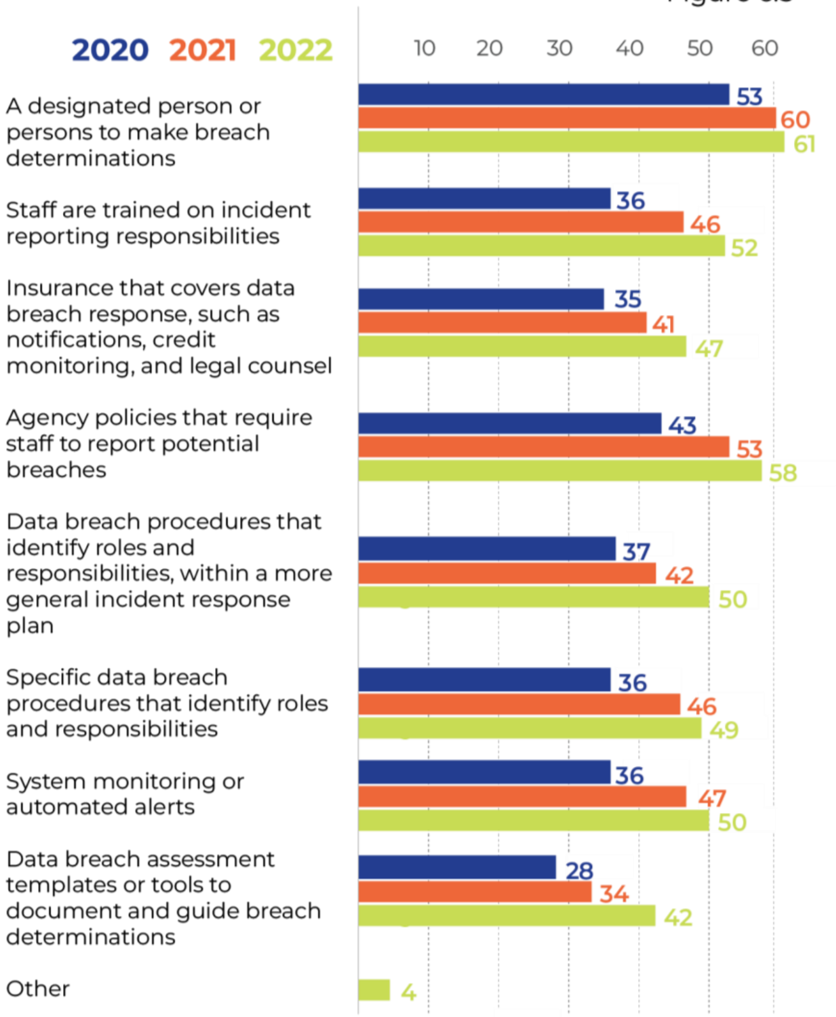
Not all incidents are cybersecurity incidents. In fact, many are not. A privacy incident is often as simple as mailing information to the wrong person or disclosing information to an unauthorized person during a phone call.

The results from the 2022 assessment were similar to 2021. A slightly smaller 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 when there is 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-one agencies, compared to 60 in 2021 and 53 in 2020, 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. Figure 6.3 shows some specific accountability measures in place at state agencies.

Figure 6.3

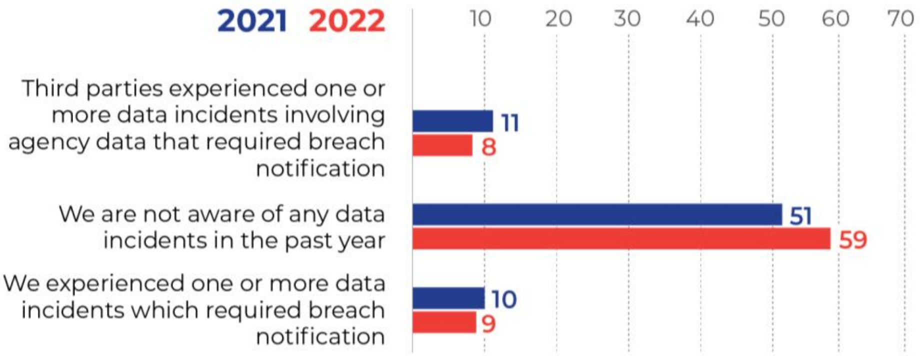


The OPDP has also expanded assistance to agencies through a Data Breach Assessment Form.docx (live.com) to determine if an incident has occurred and possible actions that should be taken.

The 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 the 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 state policy and law, including when sharing with third party vendors.

Figure 6.4 shows data from the 2022 survey regarding agency data breach incidents and third-party incidents. This chart represents the types of incidents across the whole of state government, while the next chart in figure 6.5 shows the number of agencies experiencing the specific type of incident.

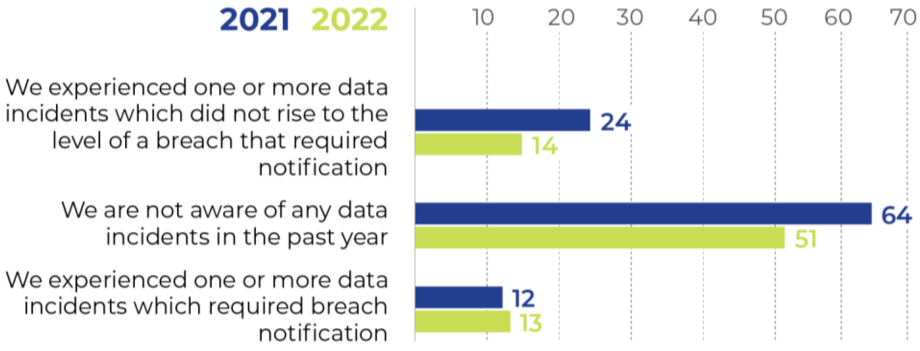
Figure 6.4



Thirteen agencies (not third parties) reported incidents that required breach notifications; 14 agencies had incidents that did not require notification; and 51 agencies reported they are not aware of any data incidents over the past year.

In 2022, 59 agencies were not aware of any third-party breaches, nine agencies knew of data breaches which did not require notification, and 8 breaches were known to require notification. All these numbers are improvements from the 2021 survey which showed more data incidents.

Figure 6.5

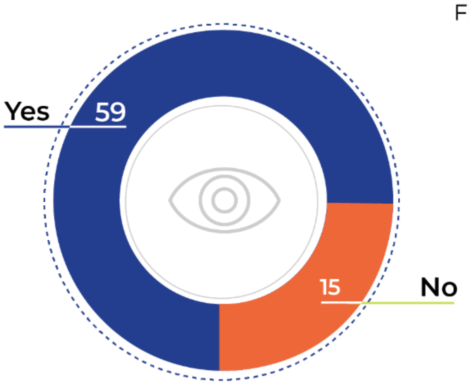


Measuring Privacy

New questions were added this year about measuring data privacy. One of the newest endeavors of the OPDP is exploring the best way to measure the maturity of privacy programs beyond this annual survey. To support this endeavor, the OPDP offered a webinar on privacy metrics.

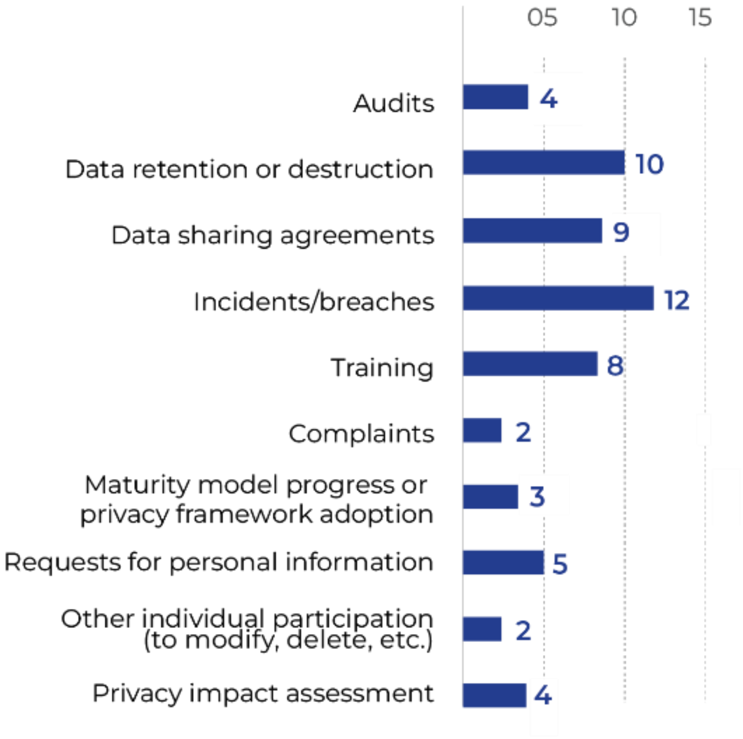
Metrics can help clarify areas of excellence (or areas that need improvement) for individual agency privacy programs and illustrate progress along the State Privacy Framework. Metrics can be tailored to individual policies and data and can show opportunities for future progress. In the 2022 survey, 59 state agencies reported that they have specific metrics related to their privacy programs. Only 15 agencies reported they do not collect metrics about their privacy programs. (See Figure 6.6.)

Figure 6.6



The OPDP looks forward to continuing to fine tune metrics, gather data across the enterprise, and use that information to continually improve privacy programs across the state. Figure 6.7 shows the types of metrics that are gathered by state agencies.

Figure 6.7



Data Sharing, Third Party Management, and Data Publishing

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.

Figure 7.1

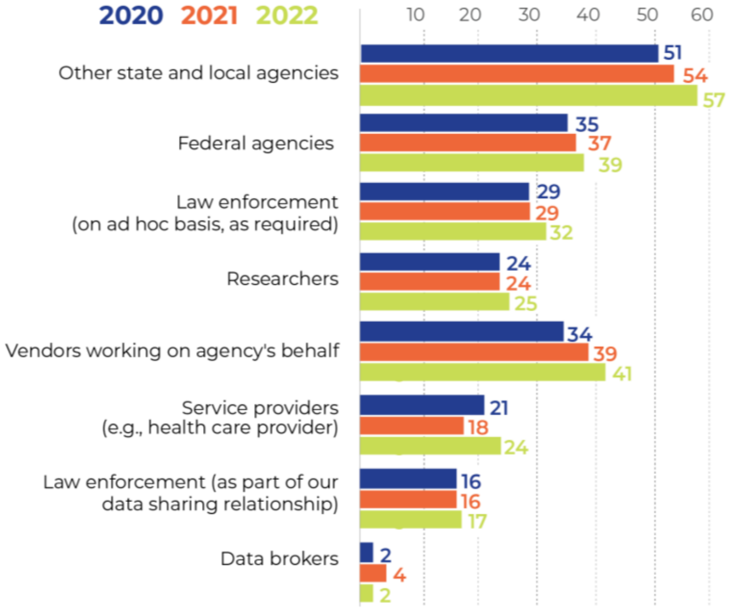


Figure 7.1 represents the entities that agencies share information with. More than 75% of agencies share personal information with other state or local agencies. The numbers represent the number of agencies that share with that category of third party. Three years of data show a trend of more data sharing, not less. Recent law has required data sharing agreements, and the OPDP has helped create model terms for those data sharing agreements for state agencies. The OPDP has also offered advice and guidance to entities developing or reviewing their data sharing agreements (DSAs).

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 developed by the OPDP for more information.

Within this data driven ecosystem of sharing, the OPDP privacy survey also asked if agencies sold data, which is different from simply sharing data through a formalized agreement. According to the survey, only two state agencies sell personal information. Over 97% of state agencies do not sell personal information.

According to the assessment:

- 52 agencies reported they have a review process to ensure contracting, privacy and security are considered before establishing a new data sharing relationship (up from 46 in 2021)
- 49 agencies have designated specific people to approve data sharing (up from 39 in 2021).
- Eight agencies have established committee to review data share requests.

Having a committee to review data sharing may not be appropriate for all agencies, but it can ensure appropriate vetting with a holistic view of an agency's data sharing relationships, within the context of the agency and the obligations it has for proper data stewardship.

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:

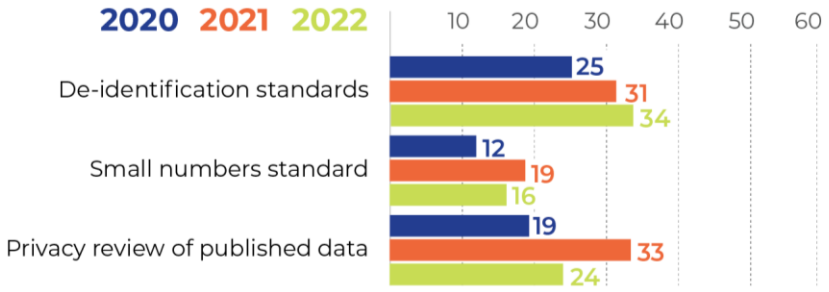
- **Creating de-identification standards.** De-identifying data requires removing more identifiers than just names. Having established standards for de-identification helps ensure appropriate and consistent practices.
- **Following a small numbers standard.** People can sometimes be re-identified when 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. A small numbers standard 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 privacy-preserving practices in place for publishing public data. Figure 7.7 shows year-to-year comparisons for these practices.

Data Sharing

State agencies are now required by state 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 State Office of Cybersecurity, OPDP and the Attorney General's Office. State agencies should continue to improve their practices to protect and maintain data in their care.

Figure 7.7

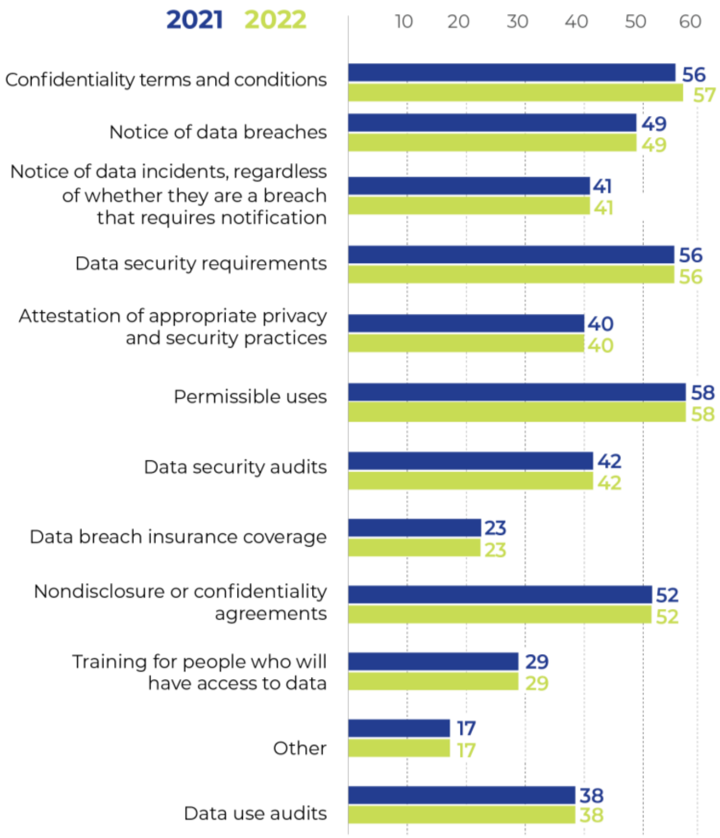


New requirements were passed into law during the 2021 legislative session that require by statute data sharing agreements that had once only been required by state policy. The new law has pushed many agencies to look for standardized agreements and best practices for data sharing agreements. The OPDP continues to contribute to this effort to better protect data through comprehensive data share agreements and adherence to the law.

To assist with this effort, the OPDP asked agencies about what was in their DSAs. Figure 7.4 offers some insight into the various elements found in different DSAs across state government. Figure 7.4 also illustrates the variance between agencies in what content was in agency data sharing agreements.

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

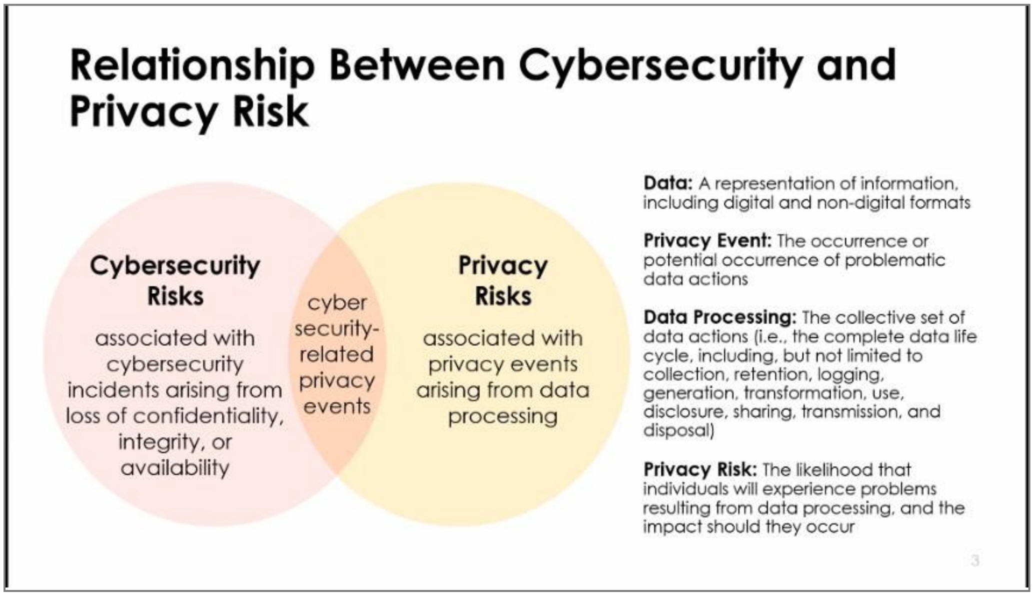
Figure 7.4



Data Inventory

Agencies often collect a variety of information from different sources and maintain it in numerous locations. Understanding what data is maintained and where it 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 it.

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 NIST Venn diagram (at right) also demonstrates the relationship between cybersecurity and


Relationship Between Cybersecurity and Privacy Risk

Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

Data: A representation of information, including digital and non-digital formats

Privacy Event: The occurrence or potential occurrence of problematic data actions

Data Processing: The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal)

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

3

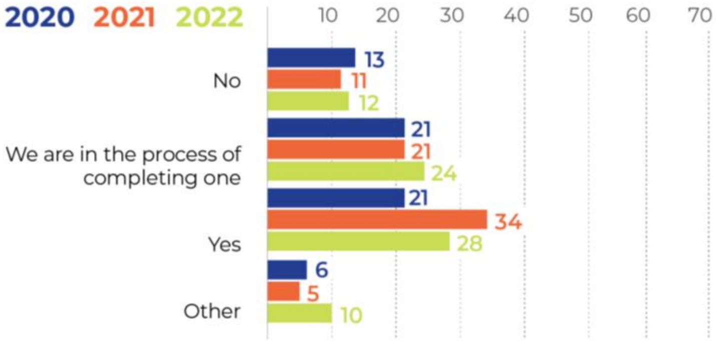
privacy for data related events due to data processing activities.

Recognizing that data inventories can be difficult to accomplish, and are often more complex than expected, OPDP asked agencies if they had completed a data map or inventory of systems and applications that includes the type of personal information maintained. Also asked was whether agencies have completed a data map or inventory that includes information stored outside of systems and applications.

Figure 8.1 shows a year-to-year comparison of agencies that have completed a data mapping or an inventory of agency systems and applications. Most notable in this data is that more agencies are in the process of completing an inventory, which shows increased awareness of the need to fully govern data.

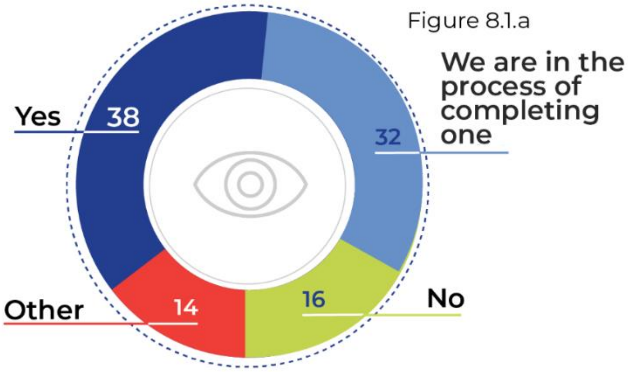
- In 2020, twenty-one agencies indicated they had completed a data map or inventory of personal information in systems and applications. This year, that number has increased to 28 agencies. This represents the fact that almost half of state agencies have done this inventory or map.
- Another 24 agencies (up from 21 in 2021) indicated they were in the process of completing one.
- In 2020, only 10 agencies had completed a data map or inventory that includes information stored outside systems or applications. That number increased to 20 (up from 16 in 2021) this year, with another 18 more reporting mapping or inventories in process.

Figure 8.1



Presenting the <u>same</u> information in a different way (percent of agencies), most - 70% - of state agencies are in the process or have done a data map. These data maps are again for data ***within*** agency systems. Figure 8.1a shows 38% of the state agencies have completed data mapping; almost 32% of agencies are in the process of completing a data mapping or data inventory process; 16% have not completed data mapping or data inventories. These percentages are very similar to the 2021 survey.

Figure 8.1.a



It is important to make distinctions between data maps of information within agencies, and outside of agency systems (i.e., vendors). The data mapping numbers change when agencies are asked about data mapping of information stored ***outside*** of agency systems. (Figures 8.2 and 8.2a). Only 27% (up from 23% in 2021) of state agencies have completed this type of data mapping of outside data. Almost 25% are currently in the process of data mapping and inventorying, and 35% (down from 44% in 2021) have not mapped or inventoried data held outside agency systems. As inventory is both a good data privacy policy and good cybersecurity policy there is room for improvement on data inventorying and mapping overall and especially for data held outside of agencies systems. All the 2022 survey results show improvement from the 2021 survey.

Figure 8.2

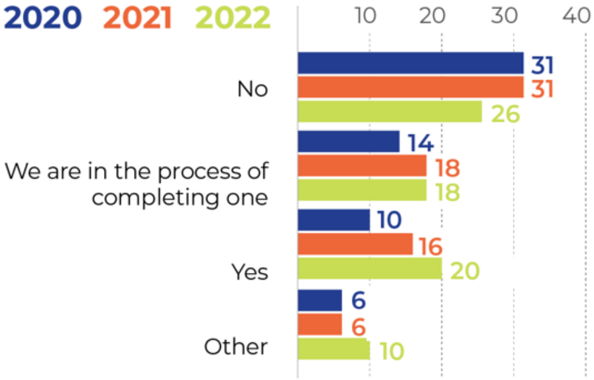
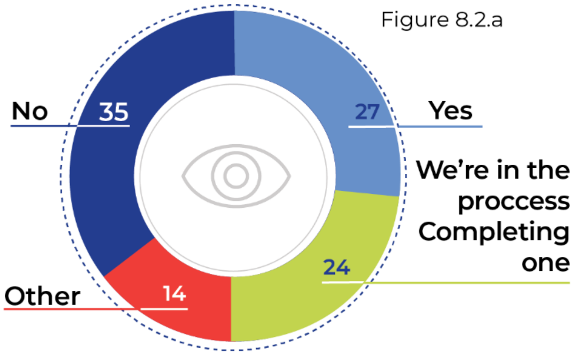


Figure 8.2.a



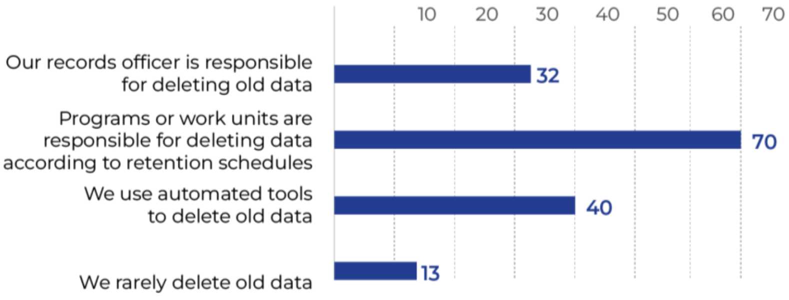
The process of data management and data inventorying offers organizations an opportunity to implement data minimization strategies and delete unneeded data. This process can also lead to cost savings and reduces risk and liability (less data means less cost to store and protect data). In asking agencies about their data inventory practices, the 2022 survey also asked about agency practices regarding data deletion as part of data minimization strategies.

Several agencies have data deletion processes in place (Figure 8.0). It should be noted that agencies that rarely delete old data may be required by statute to hold old data.

Across state government:

- 13 agencies rarely delete old data.
- 32 agencies have their records officer delete data.
- 40 agencies (same as 2021) use automated tools to delete data.
- 70 agencies (up from 64) have individual work groups or programs responsible for deletion.

Figure 8.0



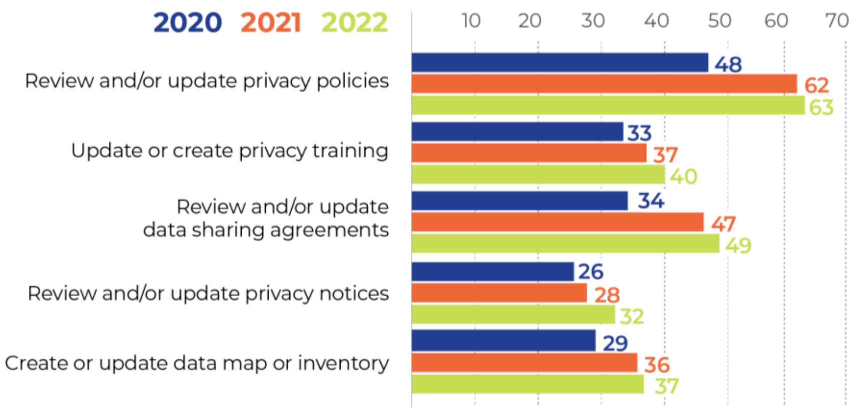
Note: agencies could choose more than one method, and so totals add up to more than 74 respondents.

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. Many agencies 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 last few years, including the review or updating of data sharing agreements. While data sharing agreement requirements have been in place as state policy for many years, attention by the Legislature and the 2021 law resulted in some renewed attention by many state agencies. Agencies have also increased participation in the OPDP webinars, trainings, and accessing other provided resources. Forty-seven agencies reported they have utilized one or more resources from the OPDP. This does not count in person, or virtual training.

Figure 9.3 illustrates data from a future looking question - What privacy tasks is your agency planning to work on in the next year? (Check all that apply)

Figure 9.3



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@watech.wa.gov.