WaTech
Washington Technology Solutions

2023 State Agency Privacy Assessment

February 1, 2024

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.

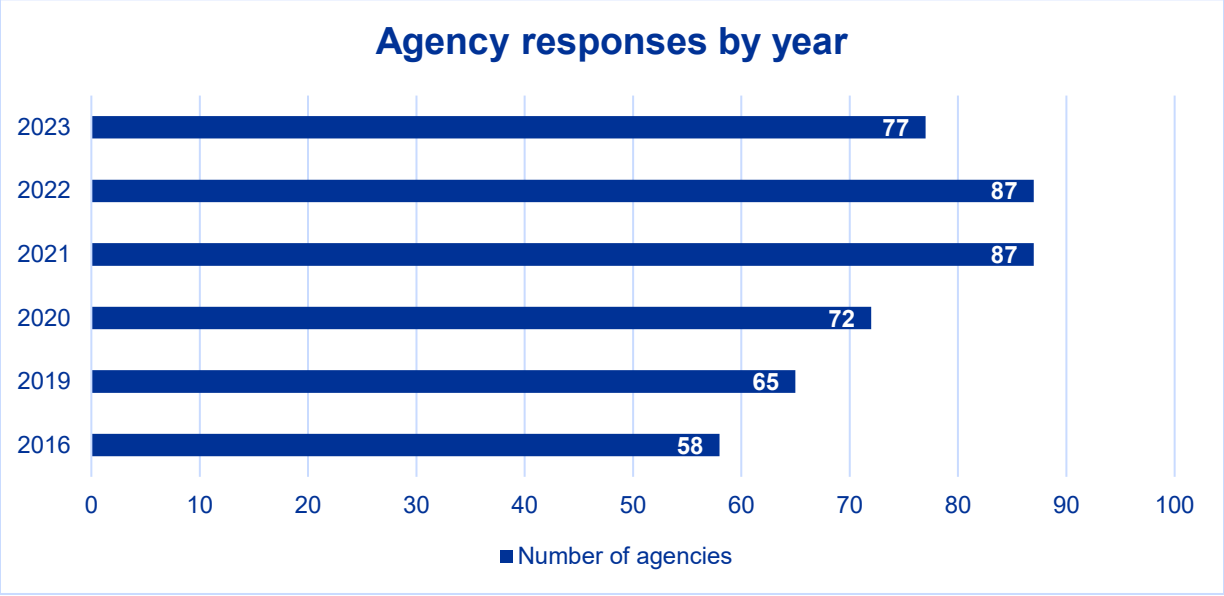
RCW 43.105.369 requires the state Office of Privacy and Data Protection (OPDP) to conduct an annual privacy review of state agency practices. The results help OPDP measure privacy maturity across agencies and develop resources and trainings where they are most needed. The goal is to establish an understanding of current practices, not to measure compliance with specific laws or standards.

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

Results from the 2023 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. There has been consistent improvement over the last four years of the survey.

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. Washington state was one of the first in the nation to develop state specific privacy prinicples and a privacy framework.

There was a slight drop off in the number of state agencies that responded to the assessment this year. One explanation for this drop in returned surveys is that the legislative branch did not complete the survey for any of its agencies due to a transition in staff. In the past, legislative branch responses accounted for close to a dozen agencies. Despite the slight drop in agencies that responded, the data offers an excellent glimpse into privacy work across state government.



Privacy maturity continues to improve across the enterprise, but work is still 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 assessment to agencies as part of the 2023 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 77 respondents, 68 agencies indicated they collect and maintain some personal information. Data in this report is based on 68 agencies. (In 2021, 72 of 87 agencies indicated they collect and maintain data. In 2022 74 of 87 agencies indicated they collect and maintain data).[1]

Personal information – also commonly referred to as personal data or personally identifiable information (PII) – is defined as information identifiable to a specific individual. The 2023 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.

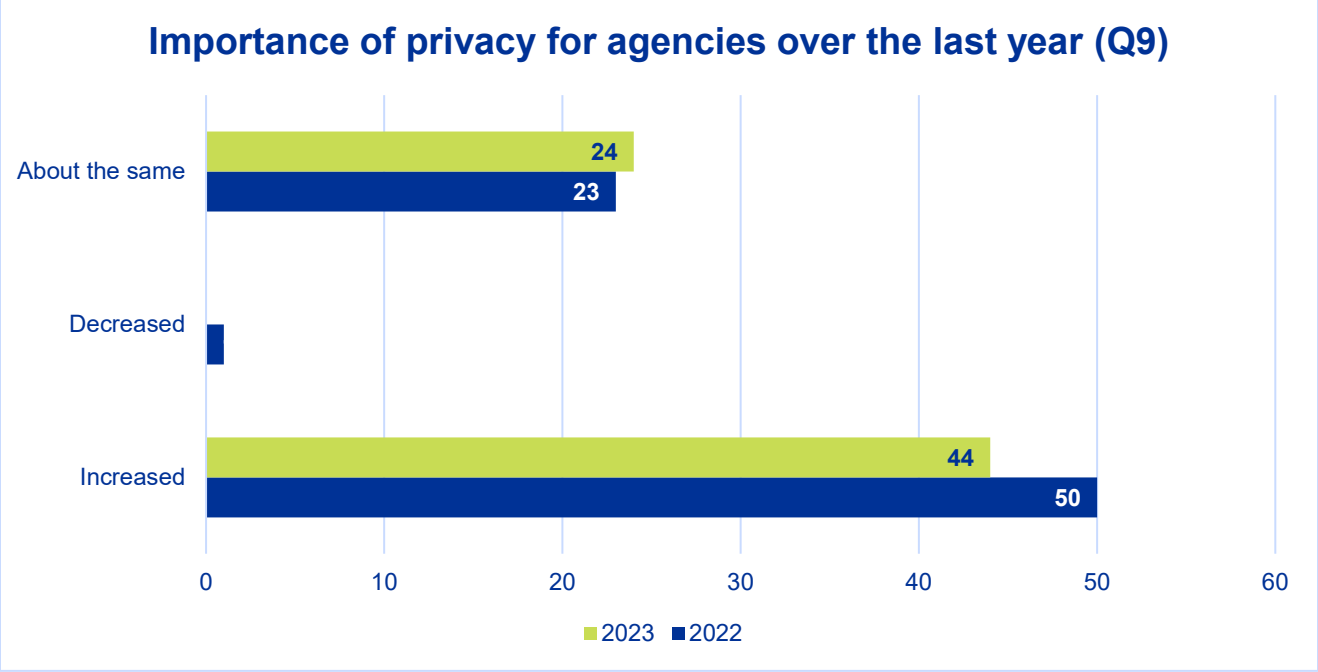
While the assessment helps gather valuable information about agency privacy practices, it is inherently quantitative. For example, it may measure whether an agency has formal policies and staff training but does not evaluate the adequacy of the policies or measure the effectiveness of the training. Data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

Many agencies in 2023 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 2022, only one agency said privacy became less important. In this year's survey, no agencies reported that privacy had become less important. Four of 68 agencies reported privacy had become more important and the rest of the agencies reported the importance was the same as in years past. This year's measurement of the importance to privacy

[1] *The nine state agencies that reported they do not hold or maintain personally identified information in the 2023 survey are: Commission on Hispanic Affairs; Columbia River Gorge Commission; Commission on African American Affairs; State Investment Board; County Road Administration Board; Transportation Improvement Board; WA LEOFF Plan 2 Retirement Board; ARTs Commission; and the Washington State Commission on Asian Pacific American Affairs.*

within the state enterprise is consistent with years past. OPDP believes 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. These trends have been ongoing for the past few years.

A note about the charts in this report. The numbers indicate the number of agencies that responded out of 68. The charts are labeled with the question number on the survey in order to cross reference the data more quickly. For example, the chart below shows answers to question nine (Q9) from the survey and shows that 44 of 68 agencies responded that privacy has increased in importance over the last year.



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, 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, especially with the increase in interest of using artificial intelligence.

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

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

OPDP also introduced 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. The privacy framework as a roadmap, illustrates that privacy maturity is an ongoing improvement process, and not a destination.

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 is intended to be a flexible and scalable starting place for agencies of varying size handling 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 the components in place but using this framework can help identify and prioritize risks and opportunities. This framework built and introduced in 2022 can also be seen as a roadmap towards better maturity for organizations.

Types of Personal Information

The first series of questions in the annual survey asked about what type of personal information state agencies maintained.[2]

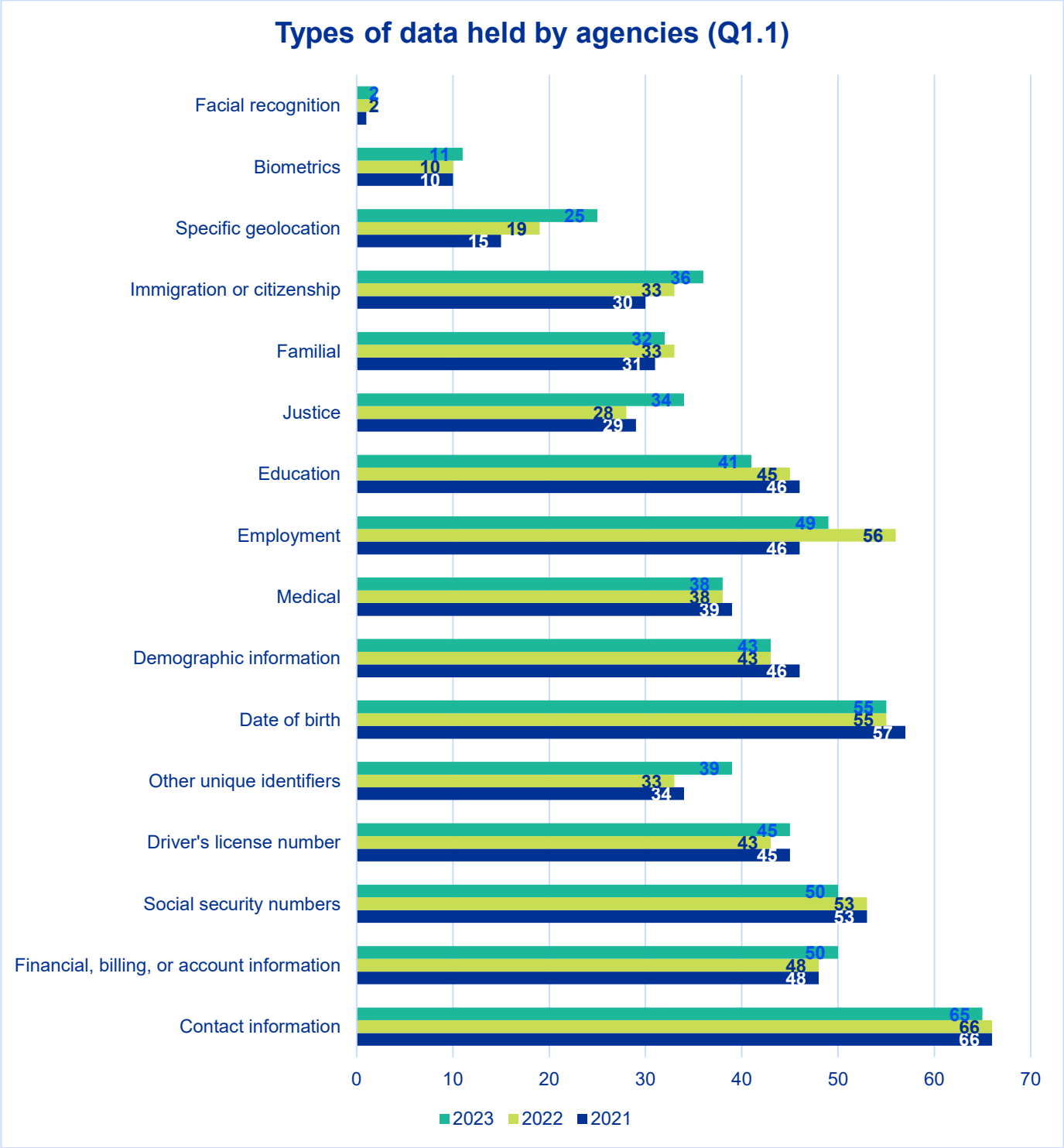
The privacy assessment gathered information from agencies about the types of personal information they maintain and the sources of that information. The assessment again revealed that many agencies maintain various types of sensitive personal information.

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. State agencies hold or maintain data due to requirements in law, or to provide services.

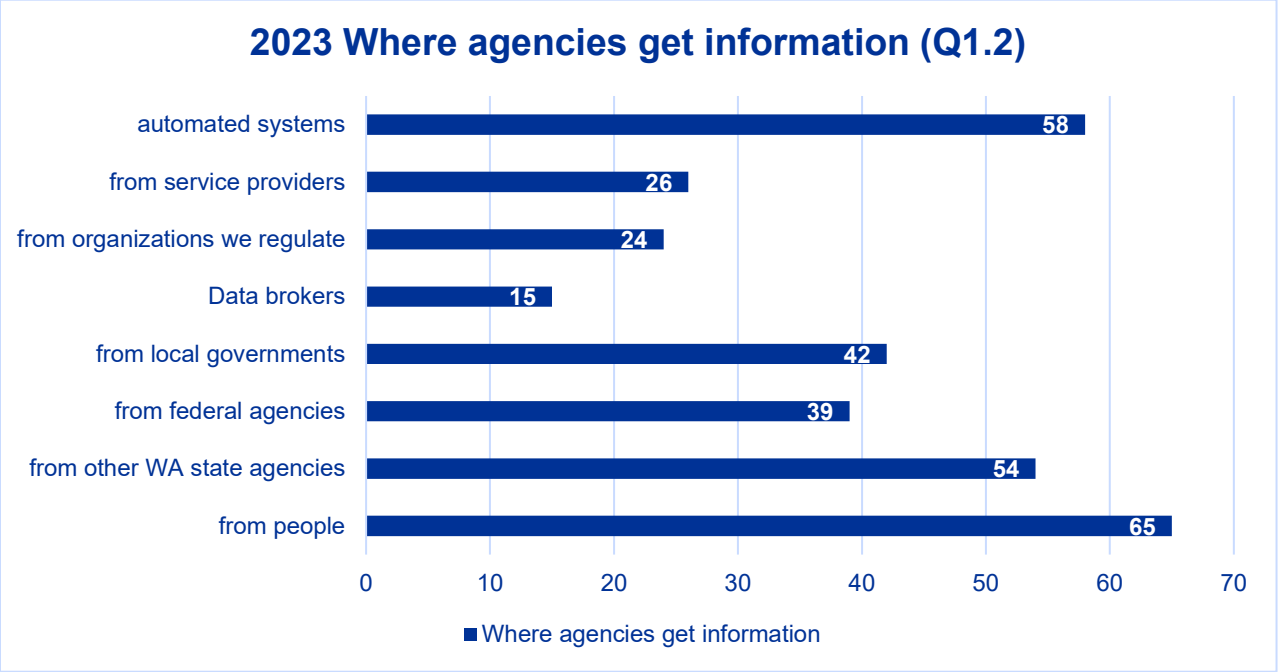
Different levels of protection are warranted for different types of information, depending on its sensitivity. State agencies hold or maintain data due to requirements in law, or to provide services. The types of information agencies have is one factor that can help determine the type of privacy controls needed to minimize risk.

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.

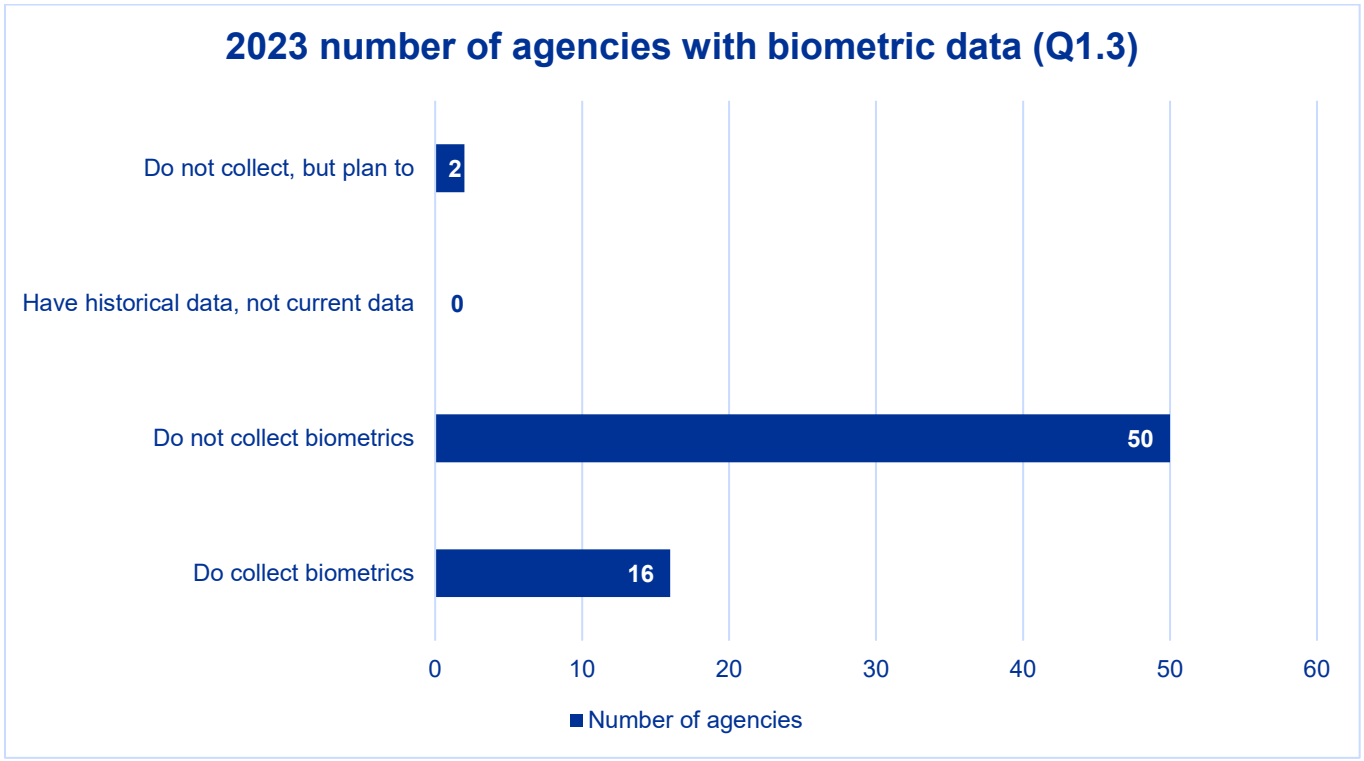
[2] *Questions: Does your agency maintain personal information about Washington residents? 1.1 What type of information does your agency maintain about Washington residents? 1.2 How does your agency collect information? 1.3 Does your agency maintain any biometric identifiers? 1.4 Does your agency use privacy impact assessments, risk registers, or other tools to assess privacy risks when beginning new projects that involve personal information?*



The types of information that agencies maintain varies widely, with most agencies holding contact information and other agencies maintaining far more sensitive information. This bar chart for question 1.1 shows how many agencies hold the most common kinds of data. The most common type of data held by agencies (65 agencies) is contact information (a number consistent with 2021 and 2022 surveys).



The next question in the survey asked where agencies get the data they hold. Sixty-five agencies reported they get the data from people (in order to provide services, or as required by law), 58 agencies reported they receive data from automated systems, and 54 agencies get their data from other Washington state government agencies.



There has been increasing interest in the policies around biometric data. In Washington state 50 of 68 agencies reported they do not collect any biometric. Sixteen of 68 agencies reported they do collect biometric data, and two agencies are currently in the process of developing standards or policies for collecting biometric data.

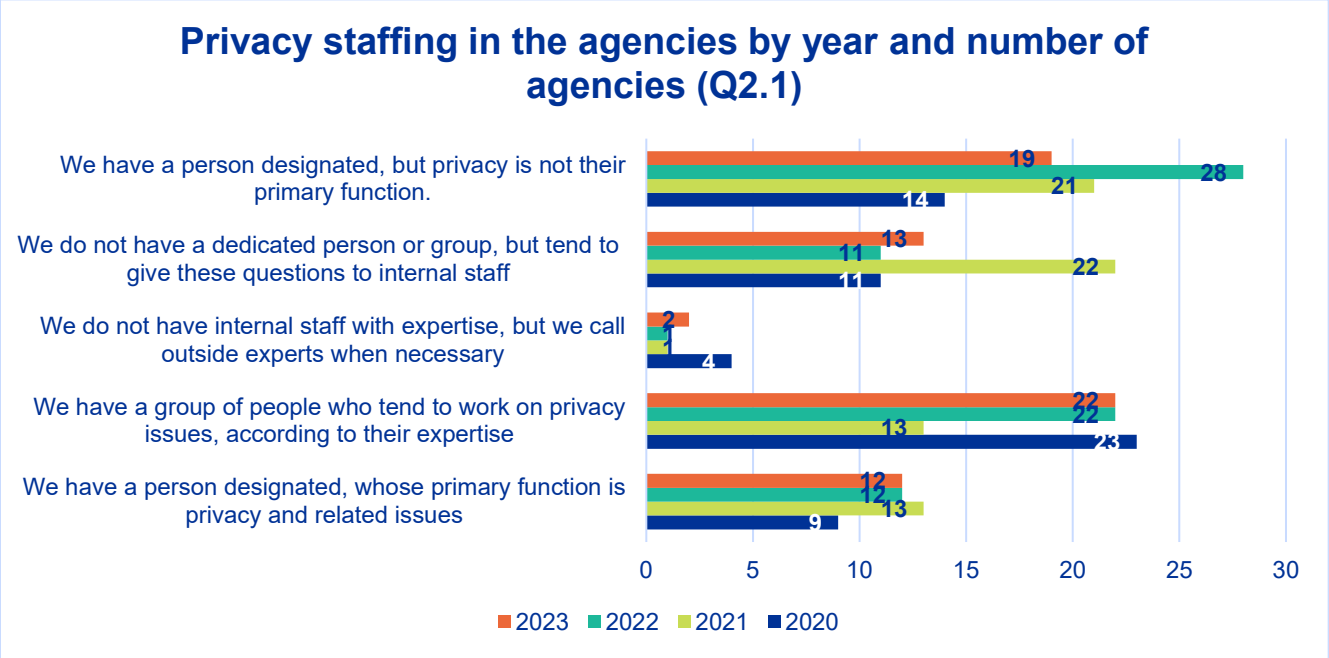
Privacy Roles and Staffing

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 staffing. 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.[3]

In 2023, 31of 68 agencies said they have a specific person designated to handle privacy policy issues (either as a primary or secondary responsibility). This is close to the same percentage of agencies having a specific person designated as in past surveys.

This chart for question 2.1 compares 2023, 2022, 2021 and OPDP 2020 survey results for staffing.



A positive metric for the enterprise is that a consistently low number of agencies are reporting that no one works on privacy for the agency. The number of agencies that do not have a dedicated person or group dropped by half in 2021 and has stayed consistent for two years in 2022 and 2023. More

[3] *Questions: 2.1 Choose the option that best describes who works on privacy in your agency: 2.2 Do you have a person designated to set policy and handle privacy questions?*

agencies across the board also report a process for handling data privacy policy questions or inquiries. Only two agencies, (down from four in 2020) reported that they depend on outside help for dealing with privacy concerns.

Having a designated person responsible for privacy is a significant step towards accountability and building a privacy program. 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 has developed and implemented training (such as the Privacy Basics Training for Washington State Employees) for the enterprise that can be utilized by personnel in any of these different disciplines – so that privacy protections can be enhanced. Dedicated staffing within agencies allows OPDP to assist customer agencies with privacy work, training, or program development.

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

For example, 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. The group is made up of state agency professionals coming from privacy, public records, legal, and cybersecurity positions.

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. The Office of Privacy and Data Protection strives to support all these individuals across state government.

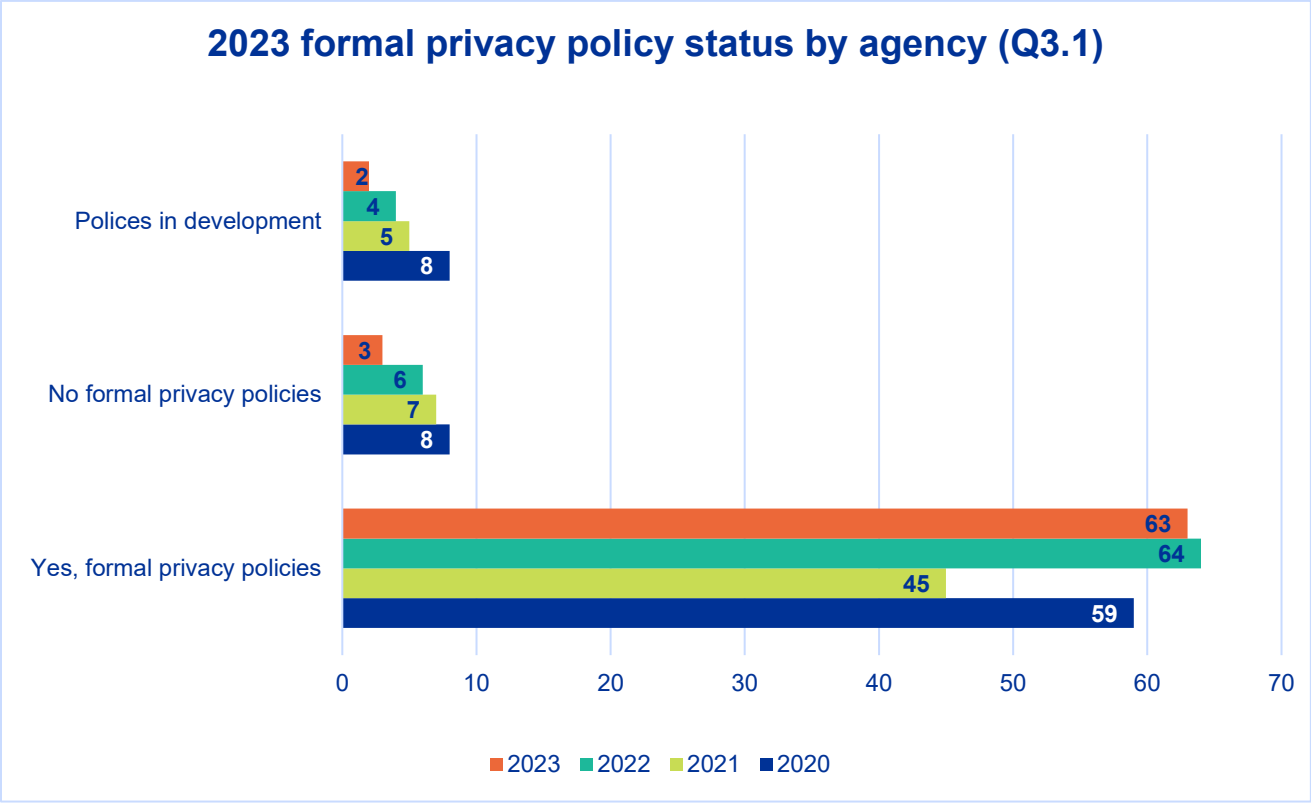
Agency Privacy Policies

Most state agencies that maintain personal data have started the process of adopting the concepts in the Washington State Privacy Principles for agency data protection. OPDP will continue to work with state agencies (and local governments) to adopt privacy principles.

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.

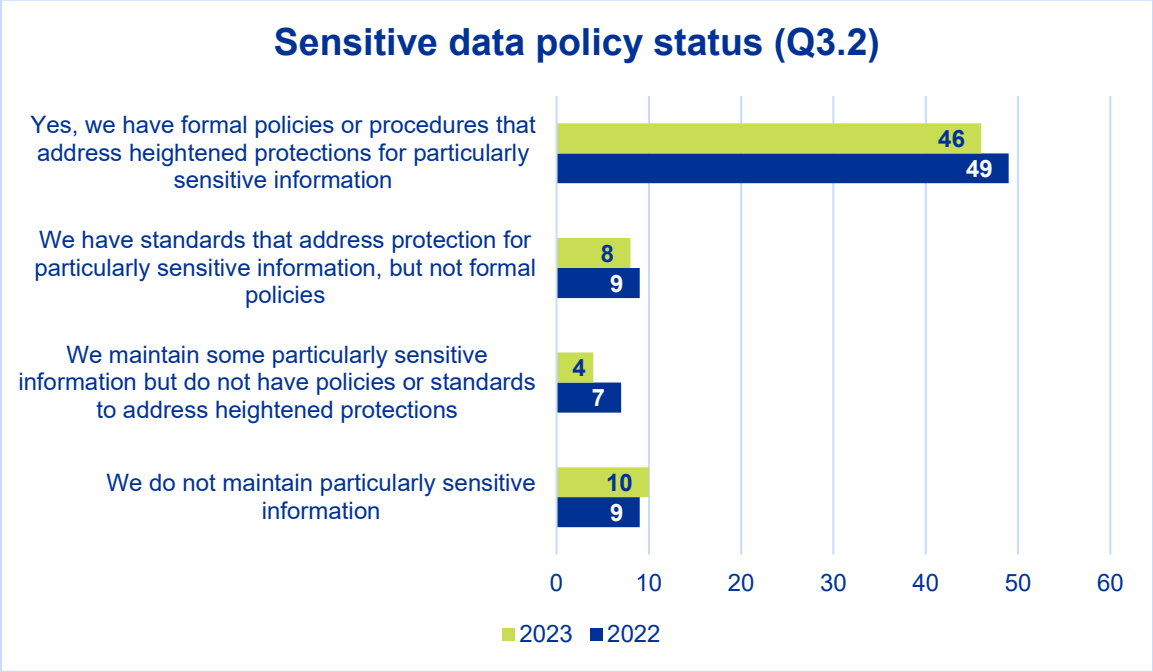
The number of state agencies that have formal privacy policies, are indicated in the chart covering question 3.1. The number of agencies without formal policies continued to shrink in 2023.[4]

There appear to be two factors driving increased formal privacy policies: 1) The increase of people working on privacy within the state government and 2) greater awareness and importance of privacy. Both factors have resulted in more policy development. Support from legislative and executive branch leadership has also helped. In 2023 more than 92% of agencies have formal policies in place, up from 87% of agencies in 2022, and 75% in 2020. The 63 agencies reporting a formal policy is up from 45 in the 2021 survey.

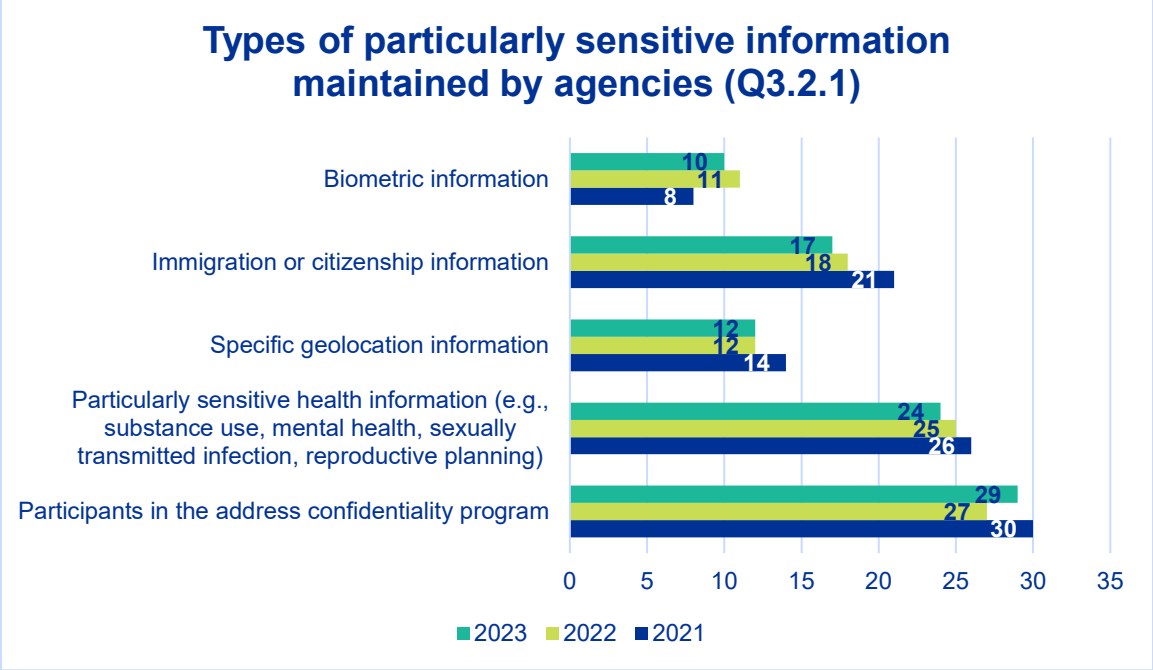


Within the general scope of privacy policies, the 2023 survey asked about specific policies around particularly sensitive information. The chart for question 3.2 (next page) shows agencies with formal policies, procedures, or other standards, that address heightened protections for particularly sensitive subsets of information. The responses between 2023, and 2022 are similar.

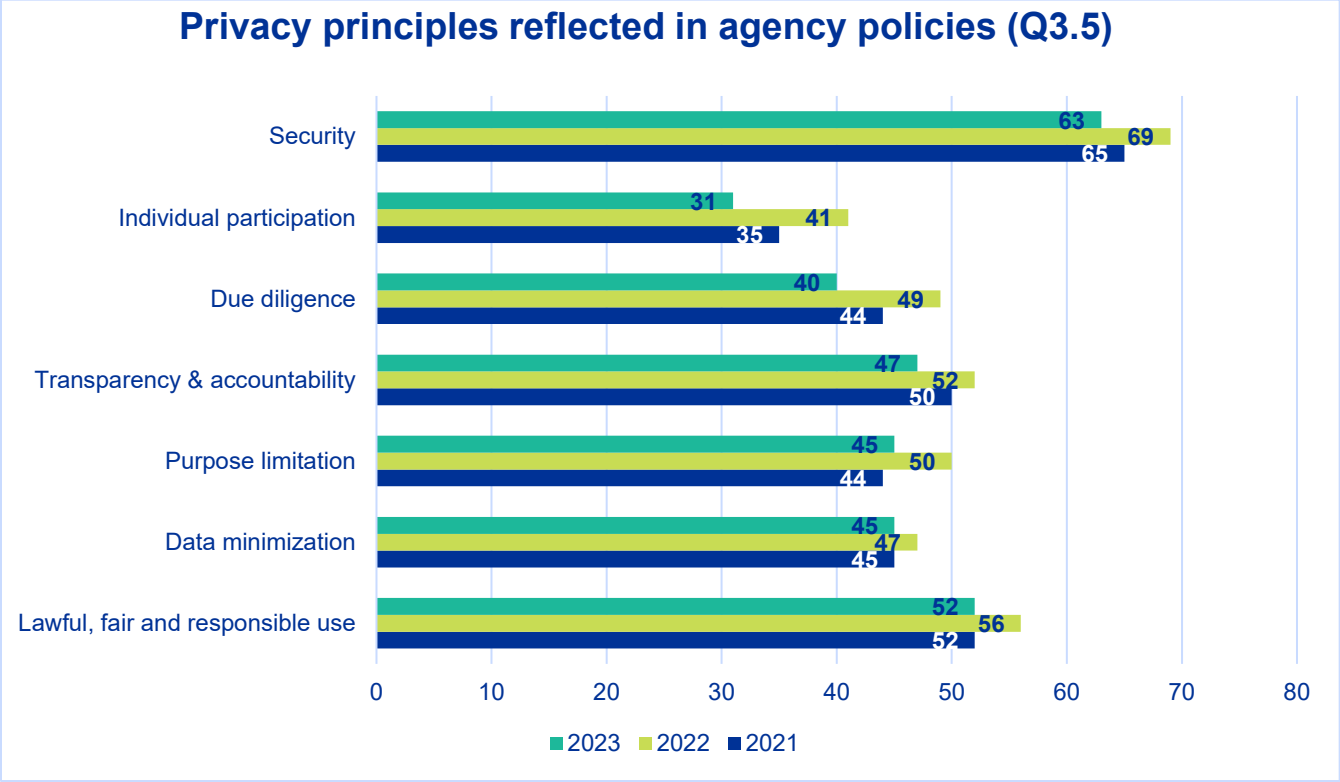
[4] *Questions: 3.1 Does your agency have formal policies and procedures that address privacy? 3.2 Does your agency have formal policies or procedures, or other standards, that address heightened protections for particularly sensitive subsets of information? 3.2.1 What types of information do the policies, procedures, or standards address? 3.3 Does your agency offer employees privacy training? 3.3.1 Is the training offered agency specific or generic training? 3.3.2 Is the training offered mandatory? 3.3.3 Does the agency utilize privacy training from: 3.4 The state Office of Privacy and Data Protection launched a general privacy training in The Learning Center called "Privacy Basics for Washington State Employees." The training takes approximately 40 minutes to take. Were you aware of this training? 3.4.1 Would you like more information about the OPDP training? 3.5 The Washington State Agency Privacy Principles are a set of fundamental principles that help guide agency practices and establish public trust. Does your agency have policies that address these principles?*



The survey drilled deeper into the kinds of data protected by policy. As illustrated in the survey question 3.2.1 chart, the specific kinds of data protected by policies, procedures or standards are clear. 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, immigration or citizenship information, as well as biometric information.



As mentioned, the state privacy principles guide specific privacy policies within state agencies. The chart for question 3.5 shows which principles are reflected in those agency policies. Year over year comparisons are consistent across the privacy principles. The "Security" privacy principle is the one principle reflected in the most agency policies or standards.



Agency Training

Staff training and privacy policies are both foundational controls that should be important pieces of any privacy program. As an office that supports the whole enterprise of state government, OPDP strives to assist with both training efforts and model privacy policies.

Training helps to ensure staff understand the importance of protecting personal information and how to implement the protection. 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.

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. The training is also being piloted to local governments that are interested.

Many state agencies have incorporated this training into their overall mandatory training for employees. This privacy 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.

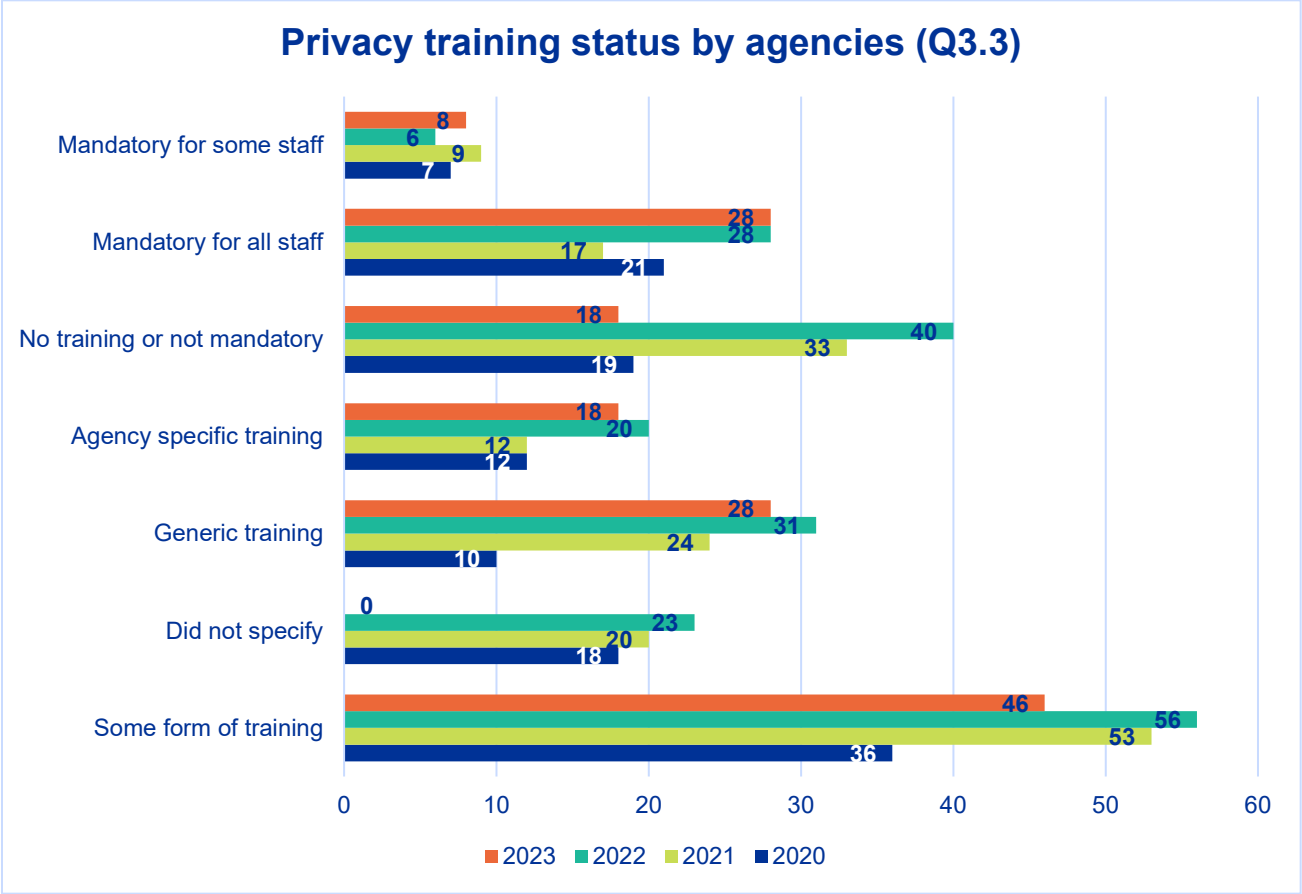
On top of web-based training, OPDP created a formal two-day workshop to support agencies and individuals practicing and applying privacy principles. It is an excellent example of how OPDP as an enterprise-focused office can efficiently provide benefits and standards for dozens of state agencies.

Agencies were asked the following questions about training in question 3.3 of the survey:

- 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?

The chart for question 3.3 plots answers from agencies across the last four years.

The 2023 responses indicate most agencies offer some form of training. This is consistent with past years data indicating more agencies offer privacy training each year. Often, privacy training is mentioned within, or is part of cybersecurity training. Standalone privacy training (either generic or specific) is beneficial to a better awareness of agency privacy policies and application of them. The number of agencies that do not offer any privacy training has continued to decline from past surveys.



Of the 46 (out of 68) agencies that offer training, 28 reported generic privacy training, and 18 reported agency-specific training. (Twenty-three 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 matched to the types of information the agency maintains and the specific policies the agency has implemented.

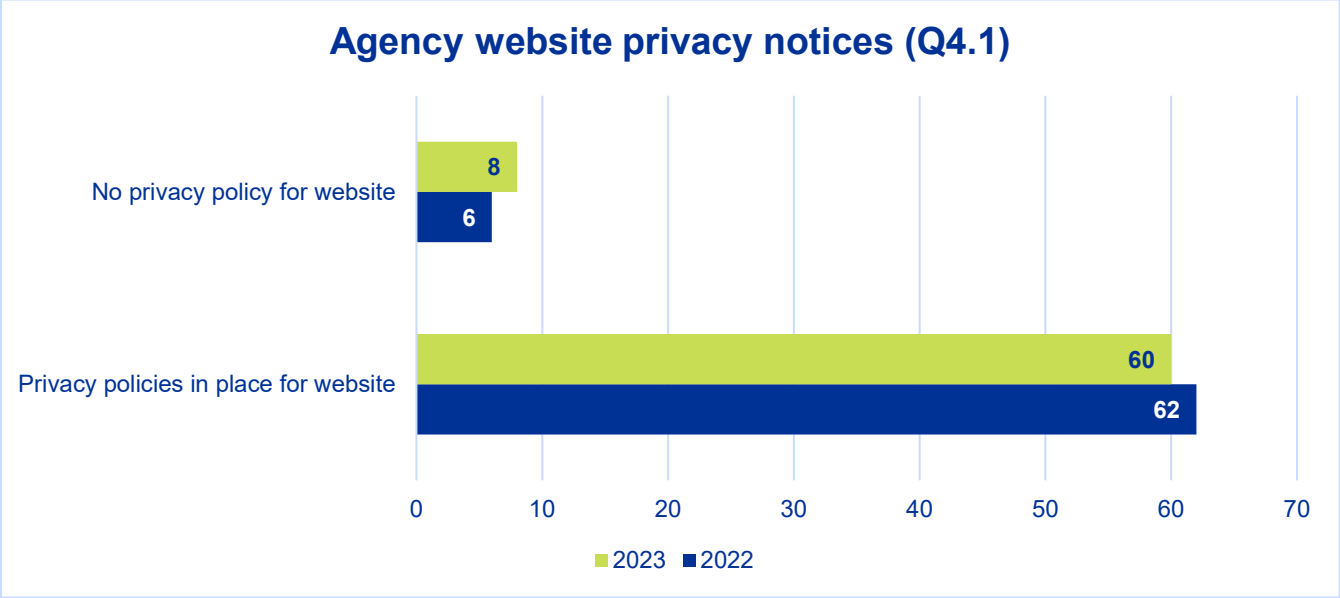
This is an area OPDP will continue to watch as the state-specific privacy training will continue to be utilized across the enterprise. The expectation is that more agencies will use OPDP training, and this area of the survey will continue to improve. OPDP prioritized creating a statewide privacy training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

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 to the public.

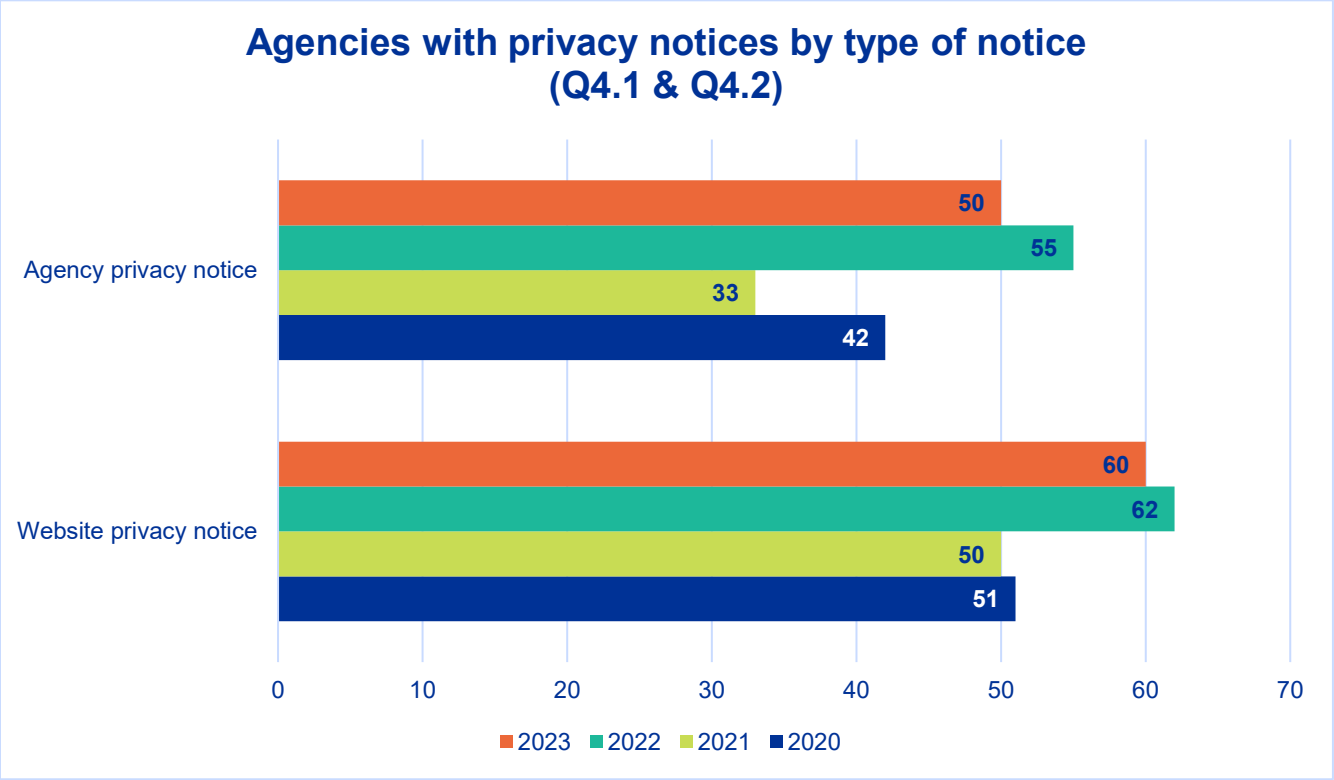
Agencies were asked about a website privacy policy, which addresses how information is gathered on the agency's website and how it is used. This type of policy addresses topics such as cookies and user tracking. Many agencies collect personal information in a variety of ways, including from online portals, paper forms, in-person, other agencies, or other third parties. This means a website privacy policy covers one way that agencies collect information about Washington residents. In 2022, 62

agencies indicated they had a website privacy policy; in 2023 it was a comparable 60 agencies indicating they have a website privacy policy (see chart for question 4.1).[5]



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 the 2023 survey, website privacy notices and agency privacy notices were measured as two policies for explaining agency data collection and use. The growth of notices is clear in the 2022 and 2023 survey data illustrated in the chart for question 4.1 and 4.2.

[5] *Questions: 4.1 Do you have a website privacy notice that addresses information you track or gather on your website? 4.1.1 How current is your website privacy notice? 4.2 Does your agency have an external-facing privacy notice that explains how you collect, use, and disclose personal information? 4.2.1 How current is your external-facing privacy notice? 4.2.2 What does your privacy notice include?*

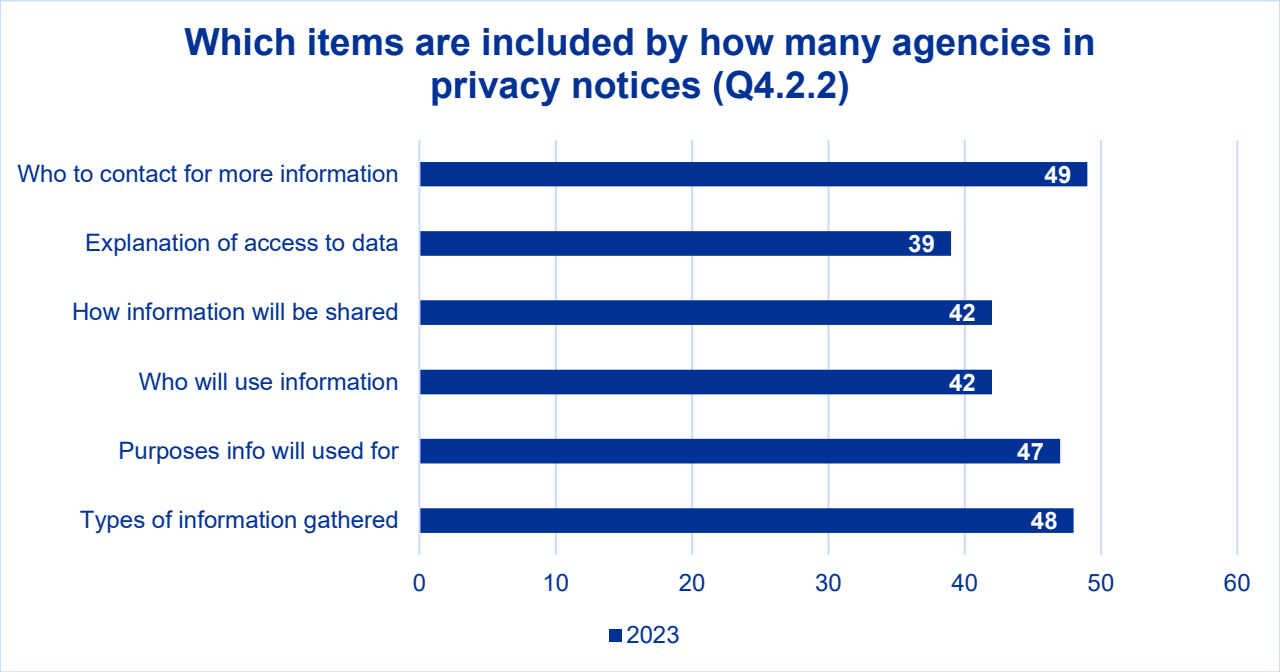


More than half of the agencies with personal information (50 of 68 agencies), indicated they have this type of comprehensive privacy notice in 2023. Most agencies post it on their website, while some also mail the notice or provide it in-person. This could be an opportunity for improvement, as many of these privacy notices have not been updated in the past year.

Agencies were 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.

The chart for question 4.2.2 illustrates the topics within the privacy policies reported by state agencies.



Individual Participation

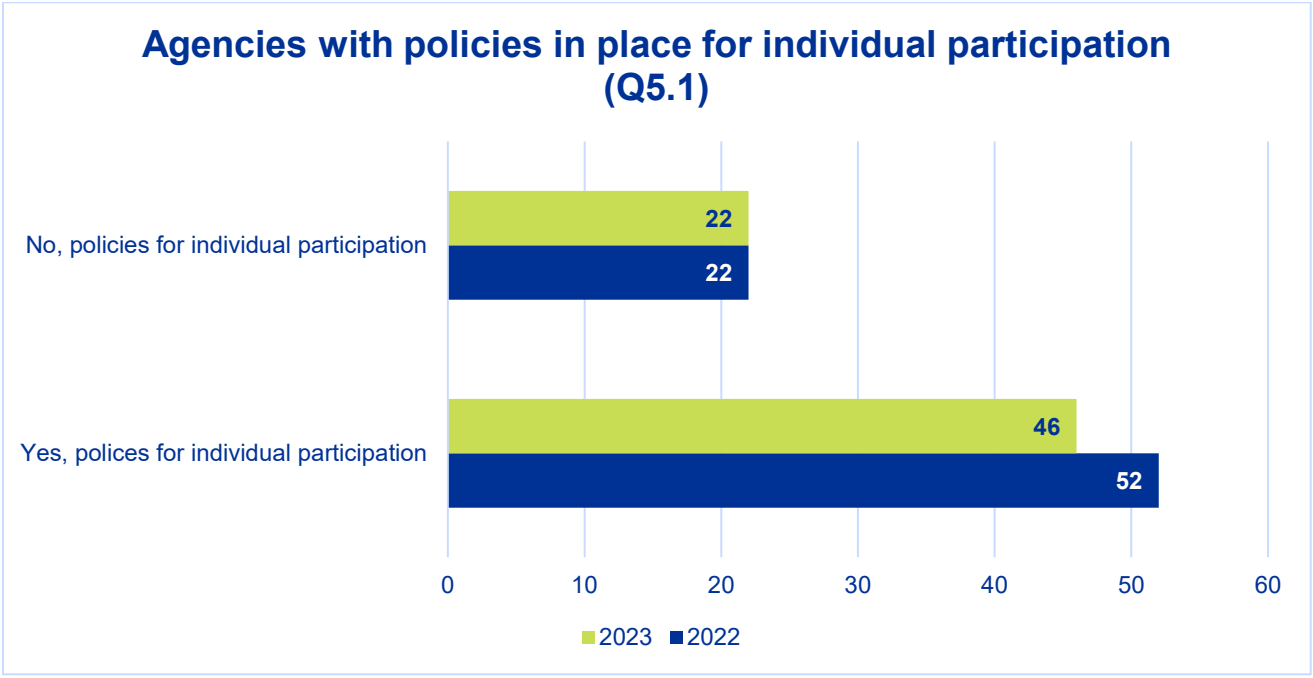
People should have control of their information whenever possible. The Individual Participation principle could be implemented by having processes for requests:

- 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.

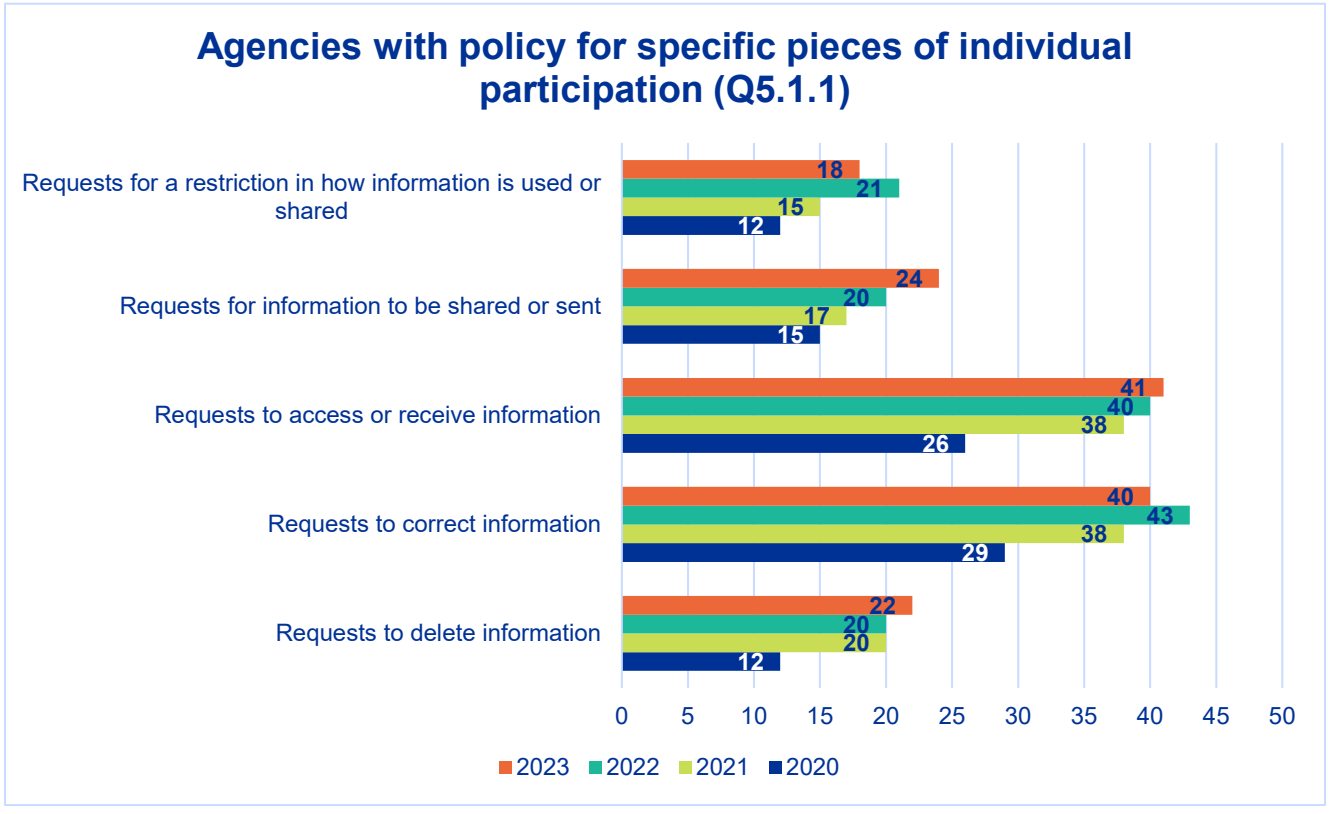
Because the government has a different relationship with Washington residents than a business has with a consumer, not all these activities are appropriate for all agencies or all government functions.

Overall, more than half of agencies indicated again in 2023, 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. Forty-six of 68 agencies reported they have at least one, (52 in 2022 and 44 in 2021) and 22 (the same as in 2022 and down from 27 in 2021) reported they do not have any procedures for individuals to control their personal data (see chart for question 5.1). [6]

[6] *Questions: 5.1 Does your agency have policies and/or procedures that address a person's request to control their personal information? 5.1.1 Which types of requests do the policies and/or procedures address?*



The chart for question 5.1.1 shows most 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 four years of survey data.



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

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.

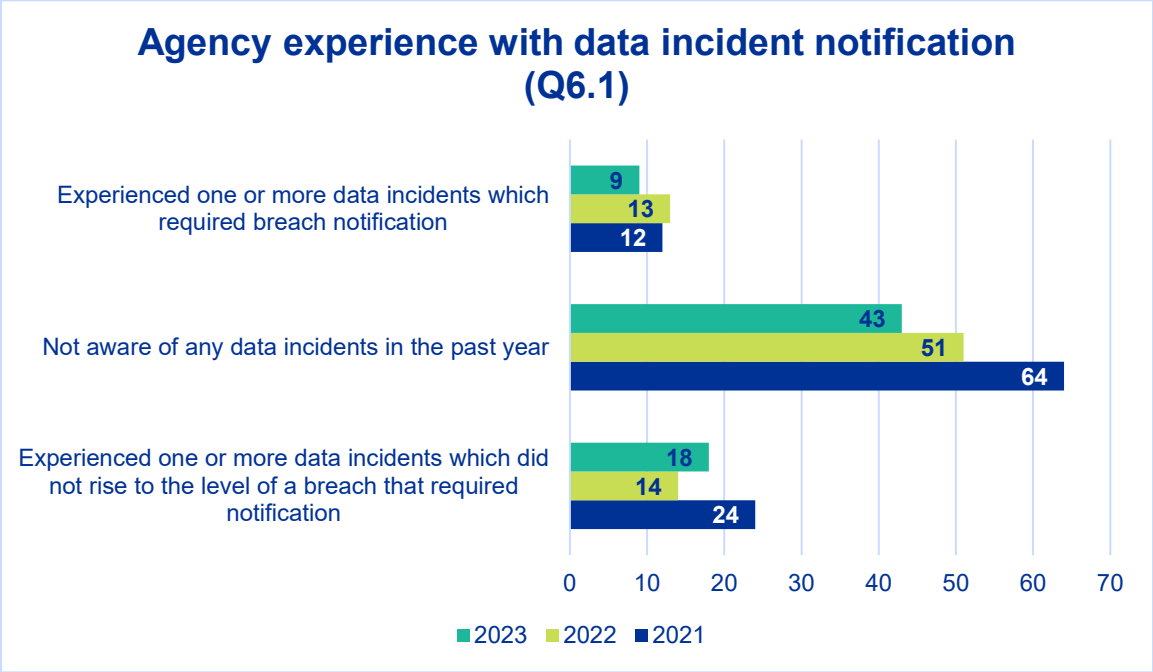
Not all incidents are cybersecurity incidents. In fact, most are not. A privacy incident is often as simple as mailing information to the wrong person or disclosing information to an unauthorized person during a phone call.

The results from the 2023 assessment were in line with both 2022 and 2021. A slightly smaller number of state agencies reported one or more incidents and one or more breaches. This data is shown in the chart for question 6.1. [7]

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 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.

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 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.

[7] *Questions: 6.1 Has your agency experienced any data incidents in the past year? An incident occurs when there is an unauthorized use or disclosure, regardless of whether it rises to the level of requiring notification. 6.2 In the past year, have third parties your agency shares data with experienced any data incidents that involved agency data? 6.3 What controls does your agency have in place to identify and respond to data incidents? 6.4 Is your agency subject to data breach notification requirements other than RCW 42.56.590? Please list or briefly describe other data breach notification requirements you must comply with (e.g., HIPAA, SSA, GLBA, etc.) 6.5 What type of security protections does your agency have in place to protect the privacy of personal information? 6.6 Does your agency collect any metrics about your privacy program? Which topics do the metrics cover?*



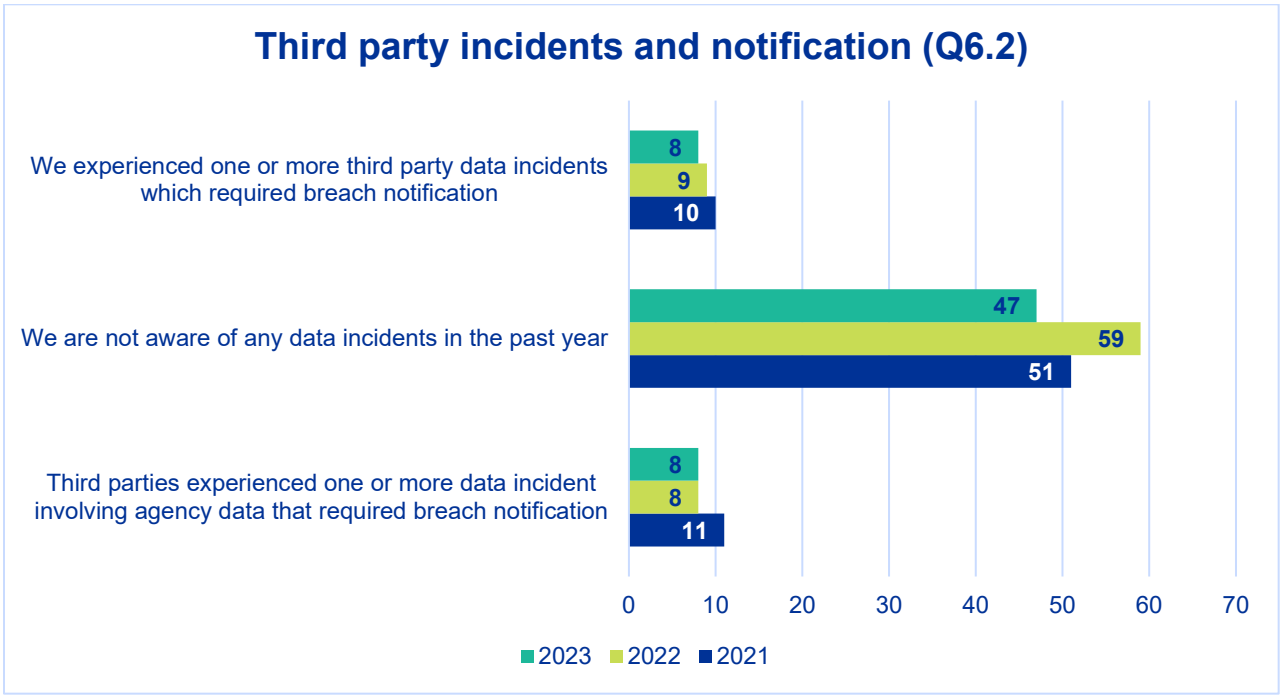
In 2023, nine agencies (down from 13 in 2022) - not third parties - reported incidents that required breach notifications; 18 agencies (up from 14 in 2022) had incidents that did not require notification; and 43 agencies reported they are not aware of any data incidents over the past year.

The Office of Privacy and Data Protection has expanded assistance to agencies through a Data Breach Assessment Form to determine if an incident has occurred and possible actions that should be taken.

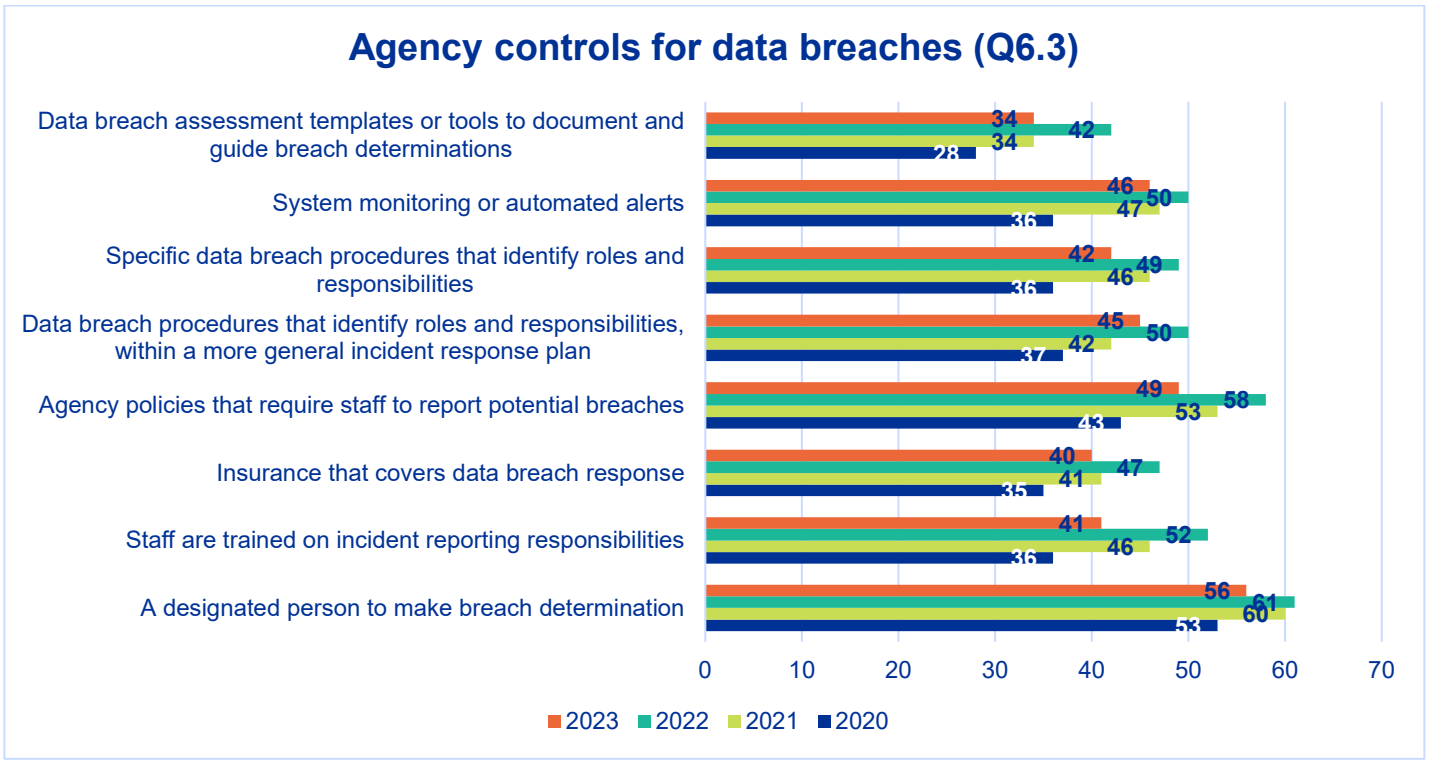
OPDP asked agencies about incidents experienced by third parties they share information with. Third parties, such as service delivery providers, technology vendors, and researchers, have significant access to personal information. Just as agencies must appropriately protect the information they maintain,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

The Office of Privacy and Data Protection has 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 chart for question 6.1 shows data from the 2023 survey regarding agency data breach incidents and the chart for question 6.2 shows data from the 2023 survey regarding third-party incidents.

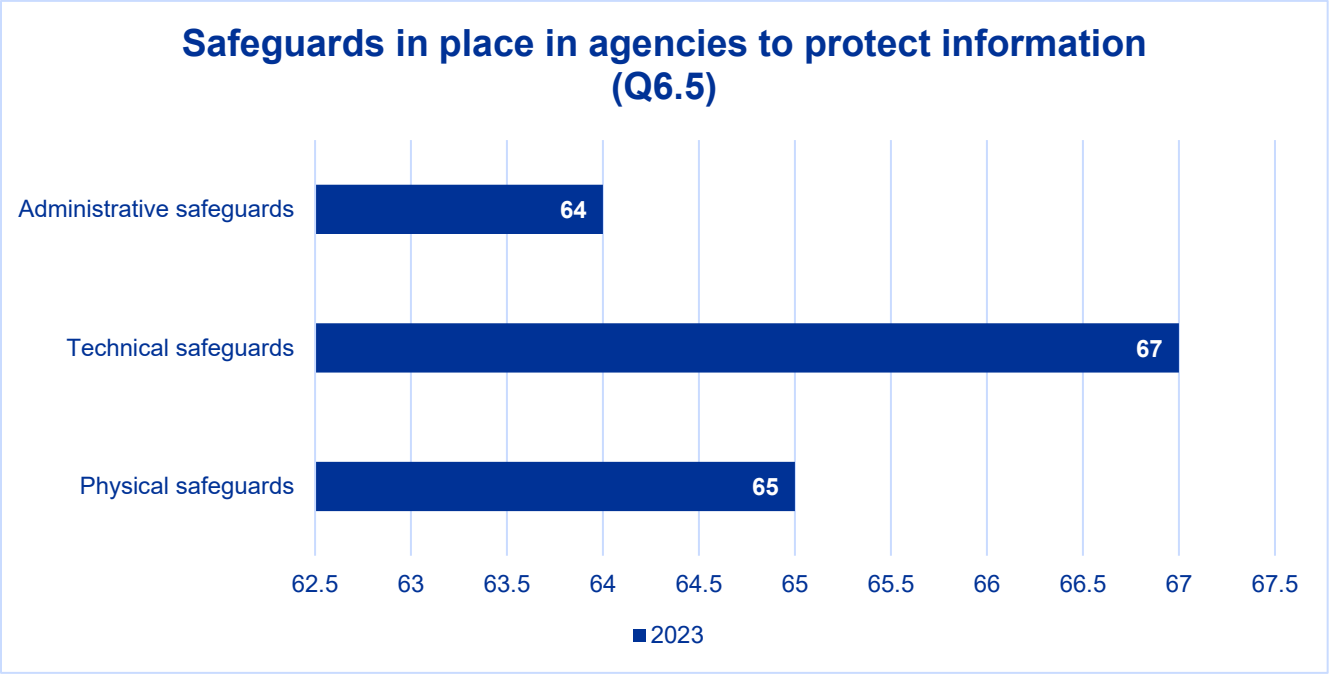


In 2023, 47 of 68 agencies were not aware of any third-party breaches, eight agencies (down from nine in 2022) knew of data incidents which did not require notification, and eight breaches were known to require notification (same as 2022). All these numbers are improvements from the 2021 survey which showed more data incidents.



We asked agencies what steps they have taken to ensure incidents are discovered. Fifty-six agencies, compared to 61 in 2022, 60 in 2021 and 53 in 2020, have designated at least one person to make breach determinations. About half of those agencies have also implemented assessment tools or templates. Overall agencies are improving in how they deal with data breaches and incidents. The chart for question 6.3 shows some specific accountability measures in place at state agencies.

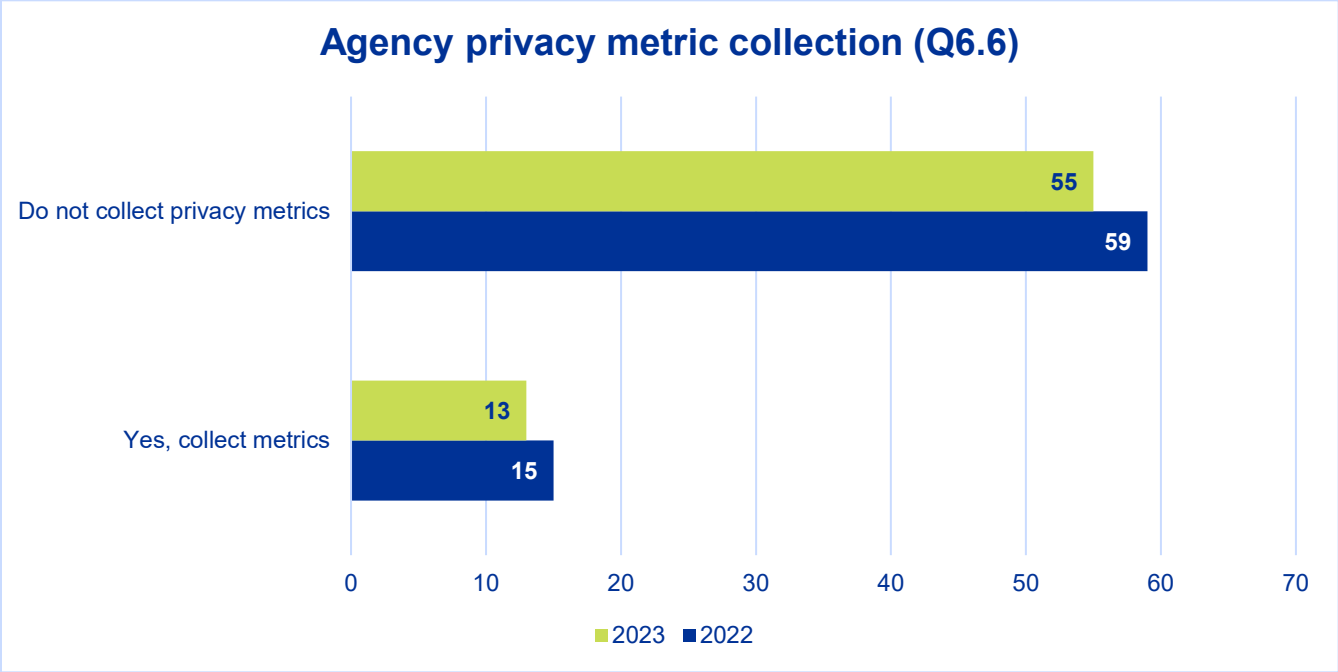
The chart for question 6.5 simplifies the breakdown of safeguards in place to protect data with state agencies. Of 68 agencies responding to the survey 64 have administrative safeguards in place, 67 have technical safeguards in place, and 65 have physical safeguards in place.



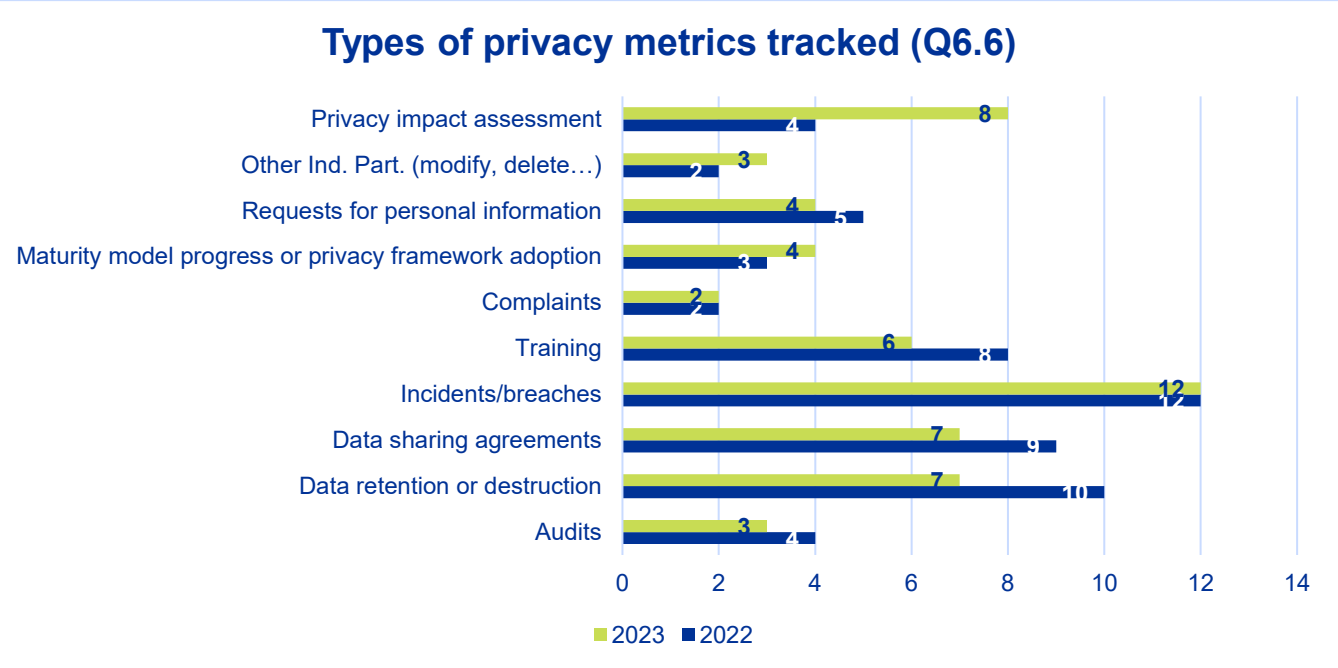
Measuring Privacy

New questions were added to the survey last year about measuring data privacy. One of the newest endeavors of OPDP is exploring the best way to measure the maturity of privacy programs beyond this annual survey. To support this, 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 do not have specific metrics related to their privacy programs. Only 15 agencies reported they do collect metrics about their privacy programs. In 2023 these numbers changed only slightly. Fifty-five state agencies reported they do not have specific metrics related to their privacy programs. Thirteen agencies in 2023 reported they do collect metrics on their privacy programs. This is reflected in the chart for question 6.6.



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. To enable that improvement the agencies that collect metrics were asked about them – as a follow up to question 6.6. Those types of metrics are shown in the chart below.



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.

The chart for question 7.1 represents the entities that agencies share information with. In 2022, more than 75% of agencies reported sharing personal information with other state or local agencies. In 2023 that number is up to 90% of reporting agencies share personal information with other state or local agencies. [8]

In the chart for question 7.1, the bars represent the number of agencies that share with that category of third party. Four years of data continue the trend of more data sharing, not less.

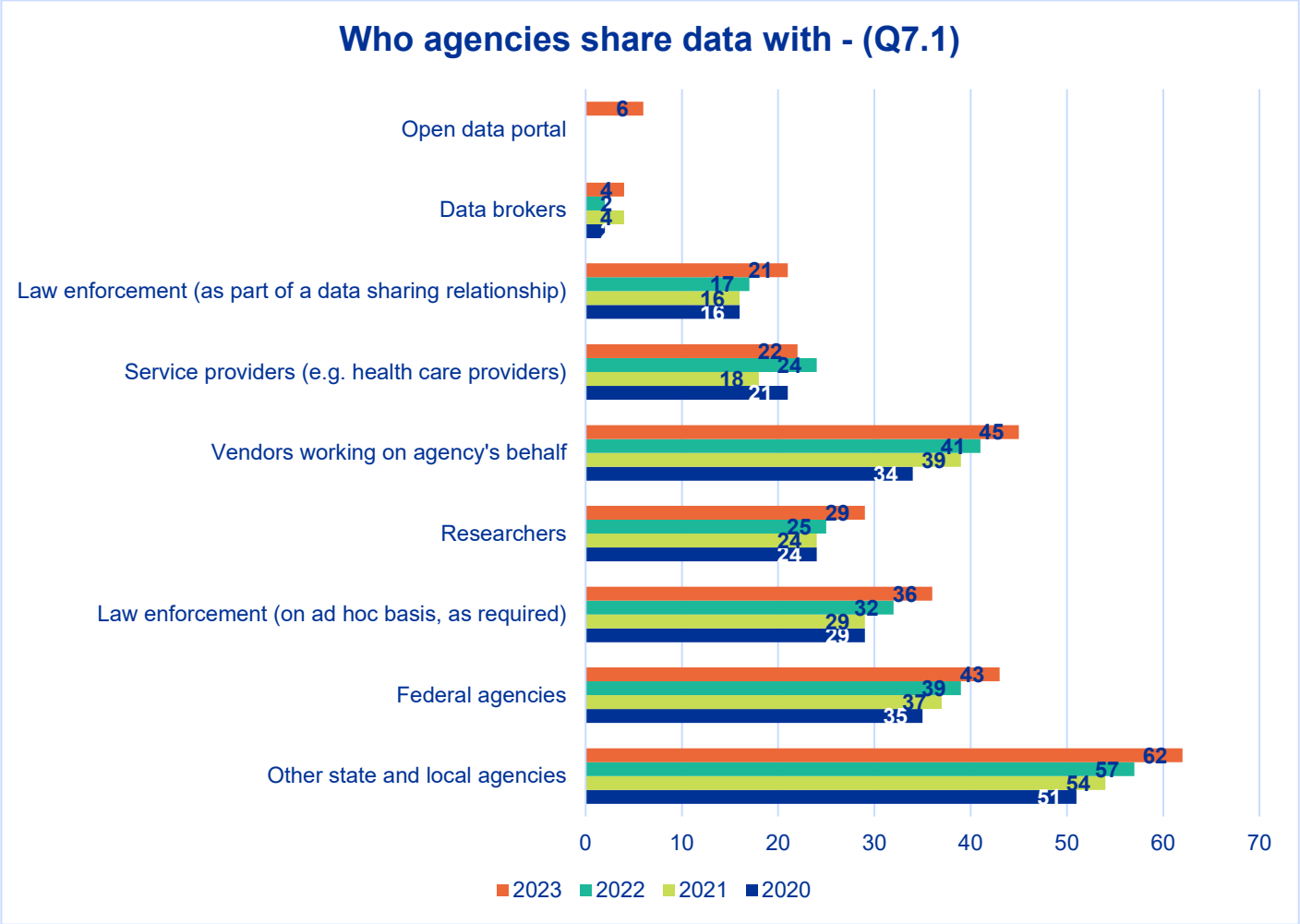
Recent legislation has required data sharing agreements for state agencies that share information, and OPDP has helped create model terms for those data sharing agreements for state agencies. OPDP has also offered advice and guidance to entities developing or reviewing their data sharing agreements (DSAs).

One new category of data sharing was added this year after discussions with agencies during the 2022 survey analysis, and 2023 survey preparation. The "open data portal" was added because six agencies reported sharing with an open data portal to provide better public access to data.

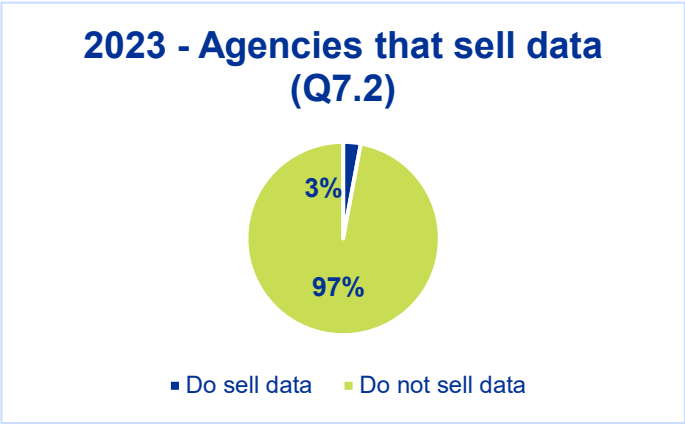
It will be interesting to watch this new metric in the future to see if more agencies share data not only with other agencies, but also with the public.

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 OPDP for more information about these controls.

[8] *Questions: 7.1 Who does your agency share personal information with? 7.2 Does your agency sell personal information? 7.3 How are requests to establish new data sharing relationships vetted? 7.4 Does your agency have processes to ensure data share agreements are in place when sharing Category 3 and Category 4 data? 7.5 Does your agency have standards or processes to minimize the risk of re-identification when information is publicly disclosed?*

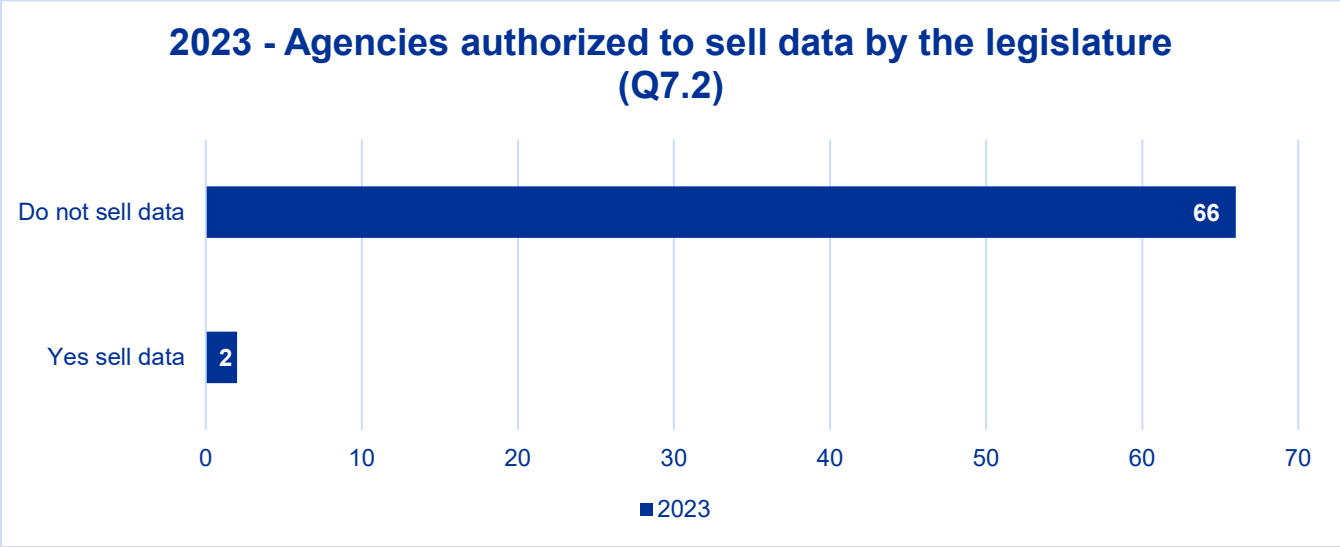


Information sharing supports efficient and effective government, but agencies should exercise due diligence both before and after sharing information. Depending on context, this may include taking steps like ensuring authority for the recipient to receive information, entering data share agreements with appropriate terms, and monitoring data protection practices. View the Data Sharing Implementation Guidance developed by OPDP for more information about these controls.



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. This information is reflected in the chart for question 7.1. This is consistent with past surveys, and agencies cited the authority to sell data granted to them by the Legislature.



Data Sharing

According to question 7.3 in the assessment (How are requests to establish new data sharing relationships vetted?):

- Forty-six of 68 agencies reported they have a review process to ensure that contracting, privacy and security are considered before establishing a new data sharing relationship (consistent with 52 in 2022 and 46 in 2021).
- Fifty of 68 agencies have designated specific people to approve data sharing (consistent with 49 in 2022 and 39 in 2021).
- Nine agencies have established a committee to review data share requests (eight committees were reported in 2022).

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, within the context of the agency and the obligations it has for proper data stewardship.

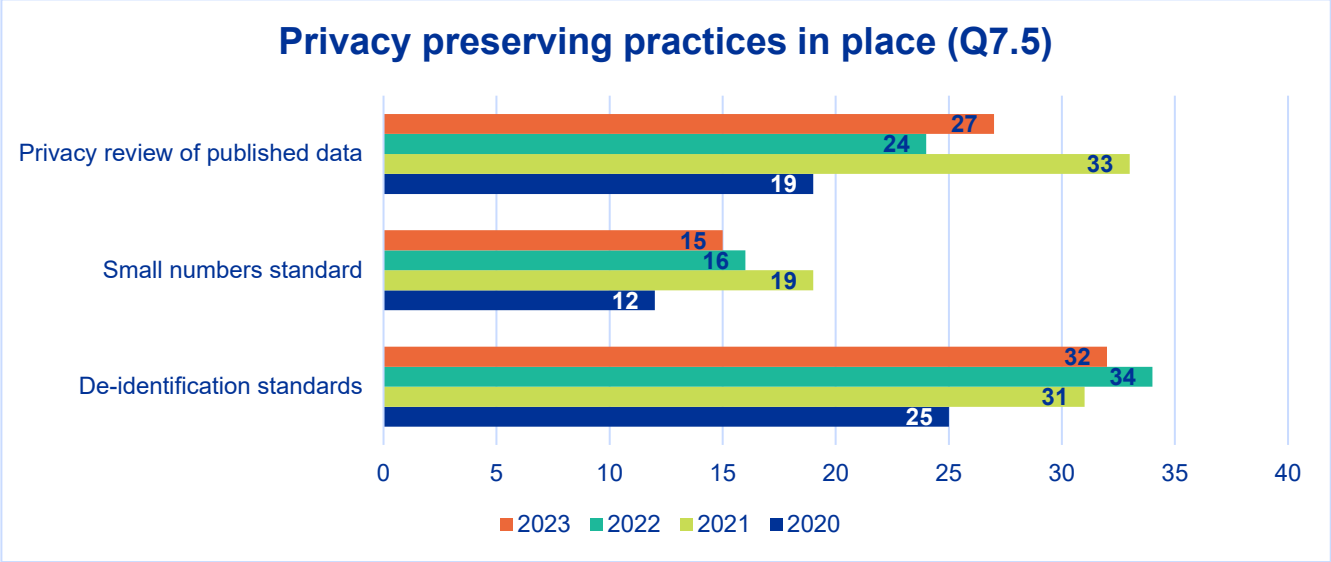
In addition to sharing personal information, agencies disclose information to remain transparent and accountable for government operations. These disclosures could include reports to the Legislature, publishing data on websites or open data portals, and sharing analysis with stakeholders. These activities 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 number of 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 privacy-preserving practices in place for publishing public data. The chart for question 7.5 shows year to year comparisons for these practices.



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 when sharing data. 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, while complying with the law.

In past surveys OPDP asked what was included in agency data sharing agreements (DSAs). That survey information informed the discussion for the legislative action, and the model DSAs offered by OPDP for state agencies. Because DSAs are now required by law, the question about DSA content was removed from the survey in 2023. The best practices and implementation guidance for state agencies can be found here:

- 2021 Cybersecurity, Privacy and Data Sharing Agreements Best Practices report
- Data Sharing Agreement Implementation Guidance

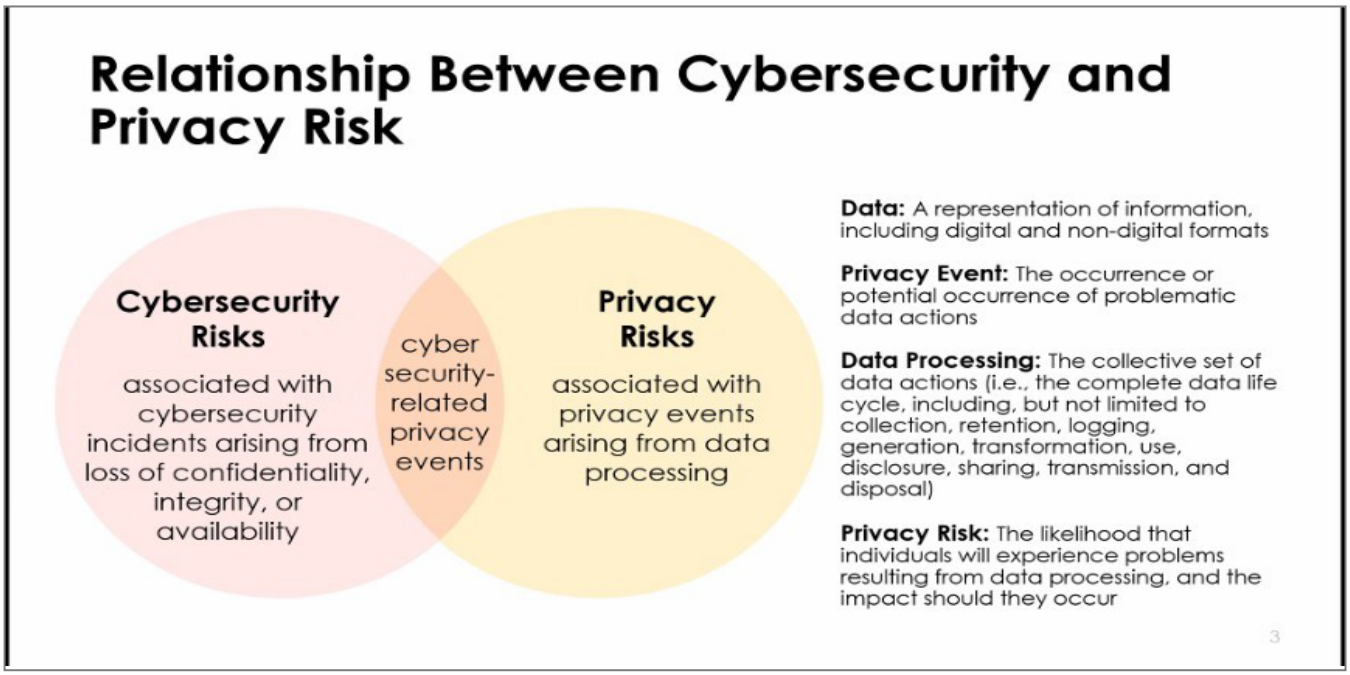
Data Inventory and Data Deletion

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 National Institute for Standards and Technology (NIST) Venn diagram (below) also demonstrates the relationship between cybersecurity and 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, the OPDP survey asked agencies about mapping data in two places – within agency systems and applications, and outside of agency systems and applications.

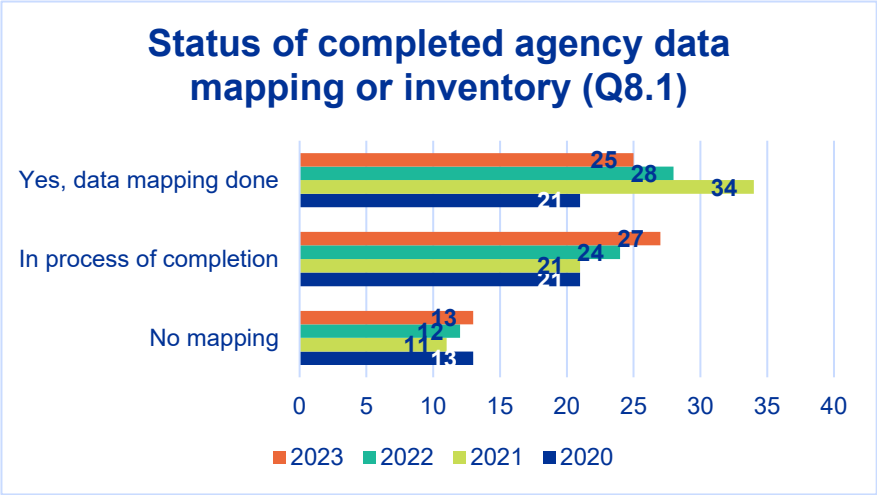
The chart for question 8.1 on page 30 shows a year-to-year comparison of agencies that have completed a data mapping or an inventory of information within agency systems and applications.

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, and a willingness to tackle the often-complex process of mapping data. [9]

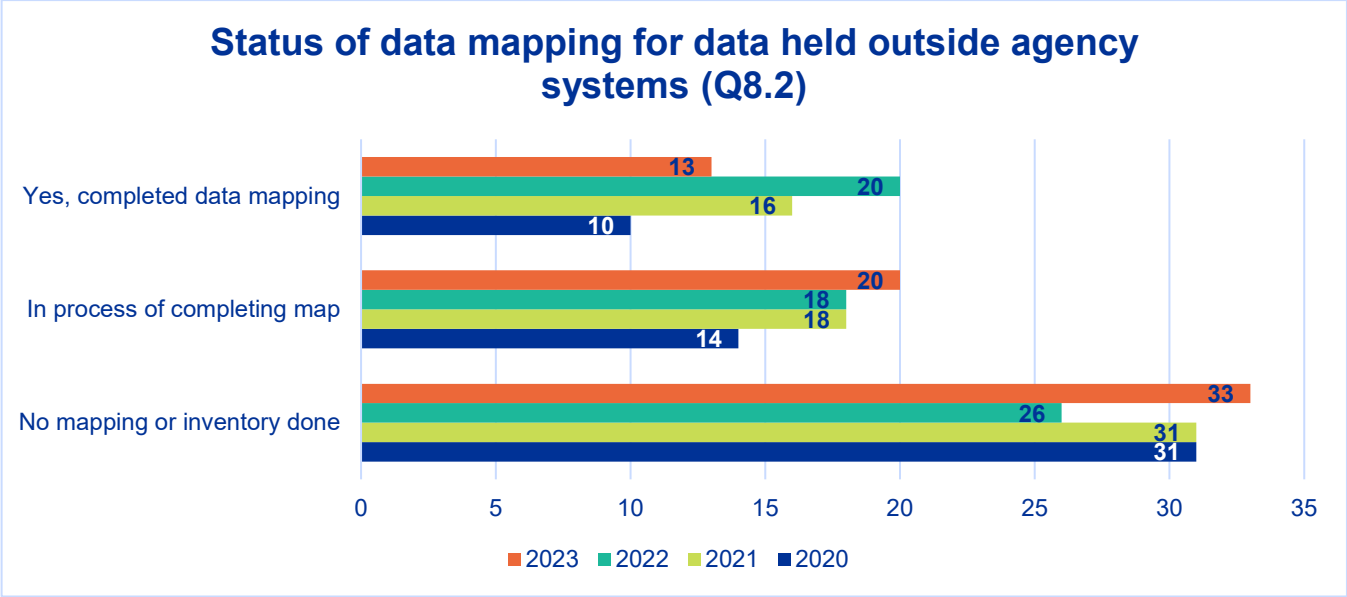
[9] *8.1 Has your agency completed data mapping or an inventory of agency systems and applications, including the types of personal information included? 8.2 Has your agency completed data mapping or an inventory that includes data or information stored outside of systems and applications? 8.3 When was your last records inventory? 8.4 How does your agency delete data?*

In 2020, 21 agencies indicated they had completed a data map or inventory of personal information in systems and applications. In 2023, that number has increased to 25 agencies reporting a completed data mapping effort.

Another 27 agencies (up from 21 in 2020 and 2021) indicated they were in the process of completing an agency systems and applications data map.



The chart of question 8.2 shows the year-to-year comparison of agencies that have completed a data mapping or inventory of information *outside* of agency systems and applications. The numbers consistently show there is room for improvement when it comes to mapping data outside agency systems or applications.



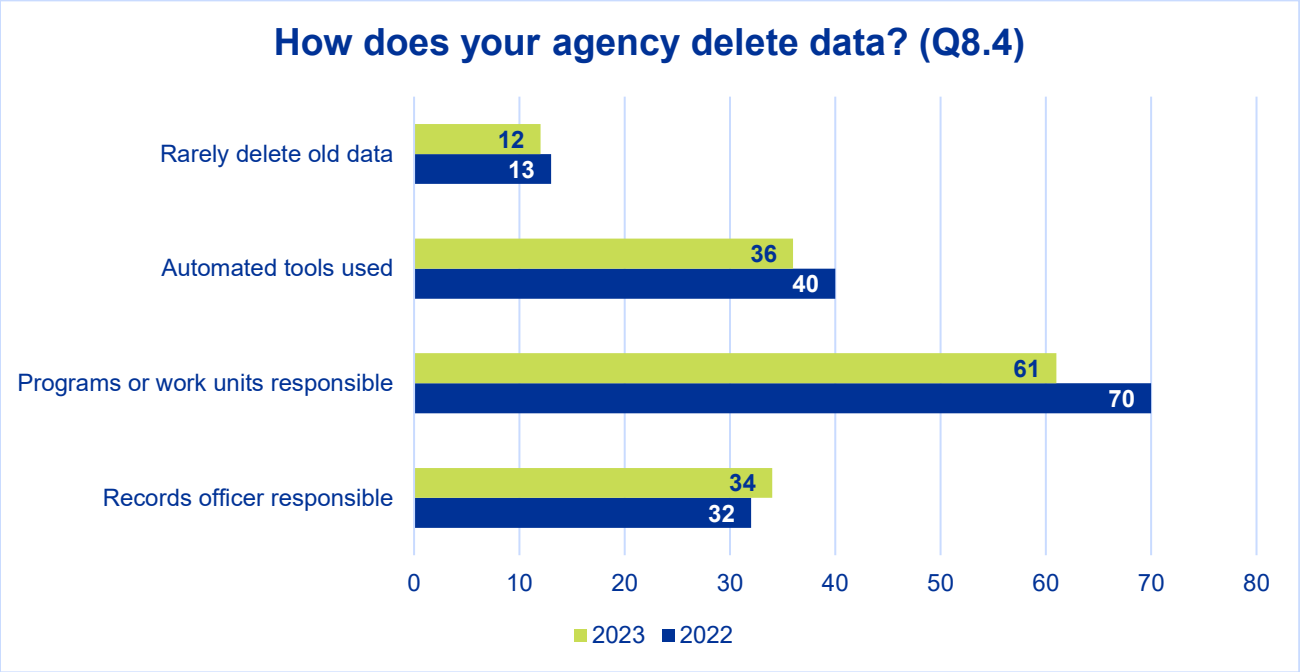
In 2020, only 10 agencies had completed a data map or inventory that includes information stored outside systems or applications. That number was consistent with 13 reporting inventories in 2023 (20 in 2022, 16 in 2021), with 20 more agencies reporting mapping or inventories in process.

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 2023 survey also asked about agency practices regarding data deletion as part of data minimization strategies.

Most agencies have data deletion processes in place as indicated by the chart for question 8.4. It should be noted that agencies that rarely delete old data may be required by statute to hold older data. In 2023, across state government:

- Twelve agencies rarely delete old data.
- Thirty-four agencies have their records officer delete data.
- Thirty-six agencies (40 in both 2022 and 2021) use automated tools to delete data.
- Sixty-one agencies (70 in 2022, 64 in 2011) 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 68 respondents.



Future Planning

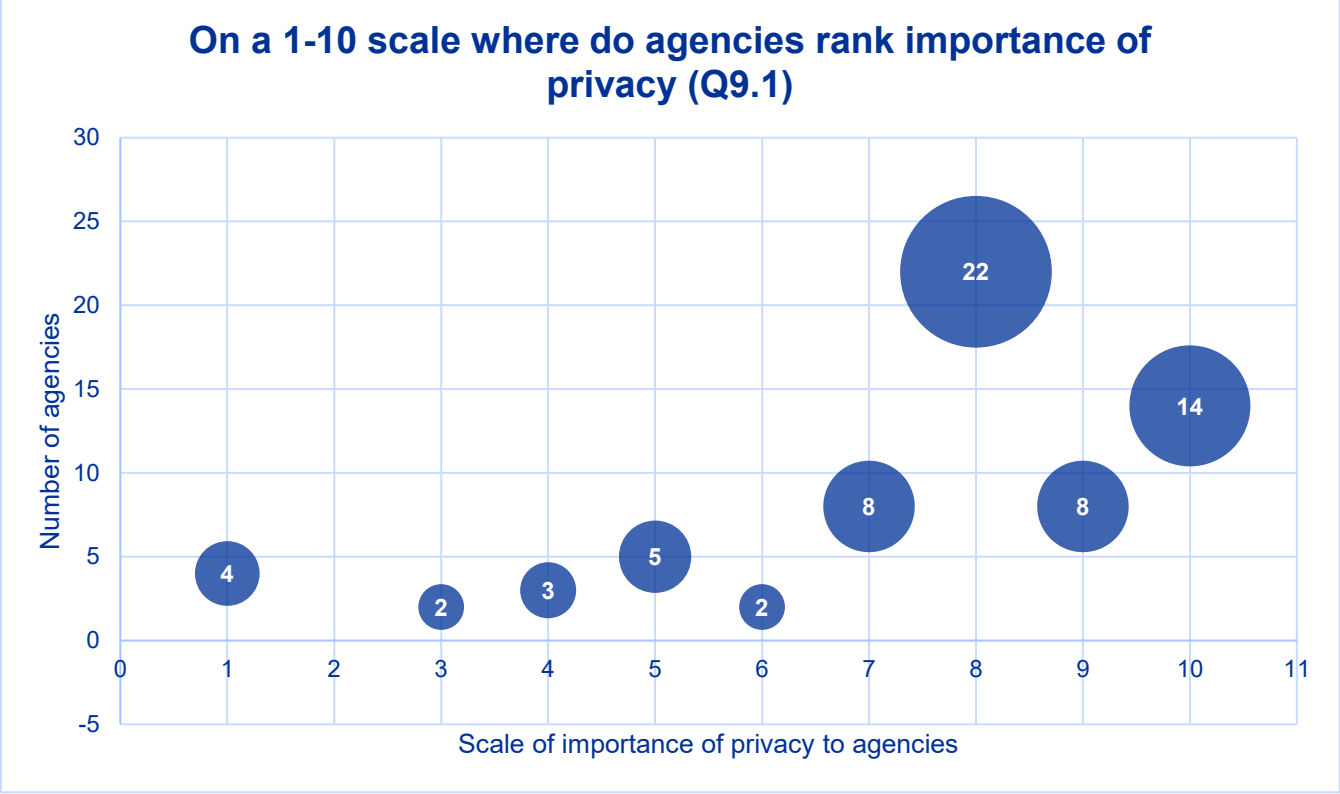
OPDP, as part of WaTech continues to focus on serving all state agencies. A portion of the annual privacy survey asks agencies about future plans to help OPDP better meet the needs of the agencies we serve.

Agencies were asked about the importance of privacy to their agency; 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.

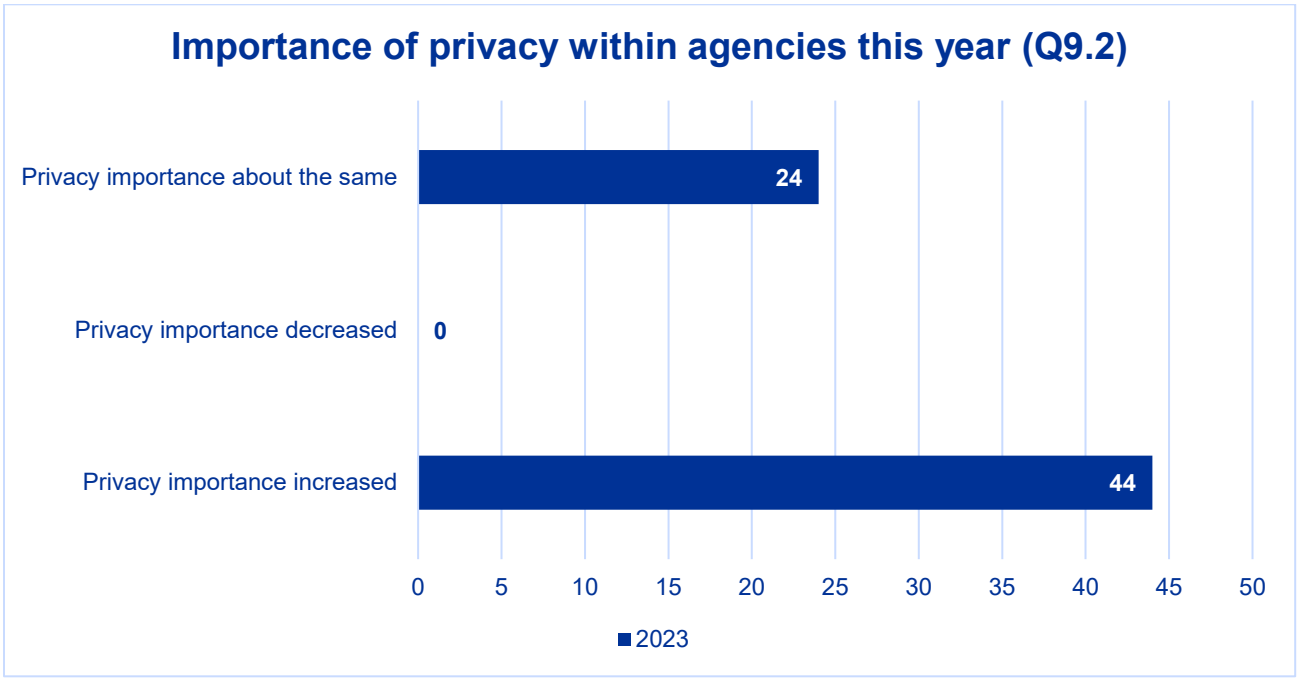
While data sharing agreement requirements have been in place as state policy for many years, attention by the Legislature resulted in some review by many state agencies. Agencies have also increased participation in OPDP webinars, trainings, and accessing other provided resources. Fifty-two of 68 (up from 47 in 2022) agencies reported they have utilized one or more resources from the OPDP website. [10]

The chart for question 9.1 shows that agencies continue to rank the importance of privacy highly on a scale of 1-10.

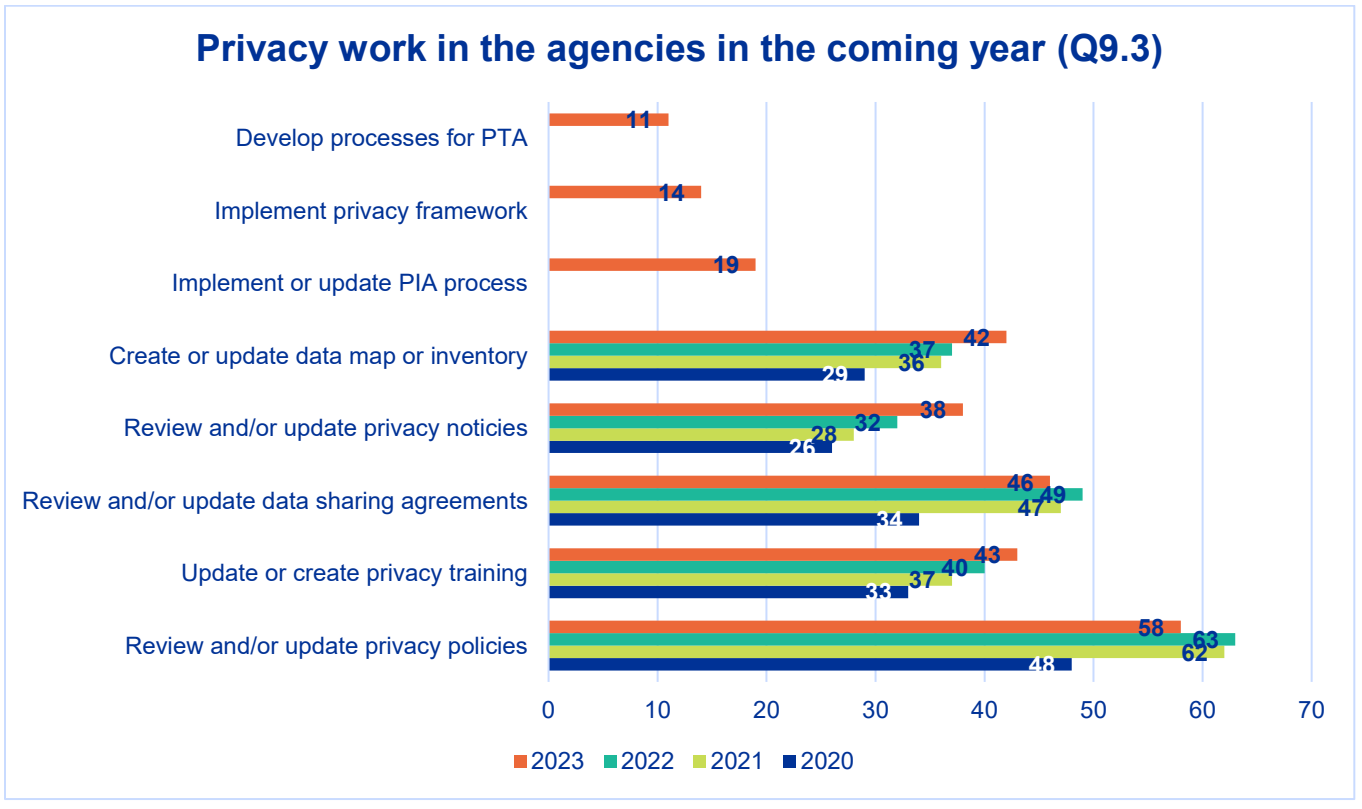


The importance of privacy is confirmed in the chart for question 9.2 which shows 44 agencies reporting that the importance of privacy has increased over the last year. No agencies reported privacy decreased in importance over the last year.

[10] *Questions: 9.1 How important is privacy for your agency this year? 9.2 Over the last two years, has the importance of strong privacy protections for your agency: Increased, decreased, stayed about the same? 9.3 What privacy tasks is your agency planning to work on in the next year? 9.4 What developments or projects most improved your agency's privacy posture in the past year? 9.5 Have you or employees from your agency attended or watched an Office of Privacy and Data Protection webinar in the last year? 9.6 Do you have suggested topics you would like to see covered in OPDP webinars in the next year? 9.7 To your knowledge, has your agency reviewed or used any of the following resources to improve its privacy and data governance practices? 9.8 What other specific resources or training topics would be helpful to your agency? 9.9 What was your level of satisfaction in your interactions with OPDP over the past year? 9.10 Please share any other thoughts or suggestions based on your interactions with OPDP.*



The chart for question 9.3 illustrates the expected privacy activities agencies are currently planning. In 2023, OPDP updated the options on this question and included the important work of Privacy Threshold Analysis, implementing the Washington State Privacy Framework, and Privacy Impact Assessments.



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.