WaTech
Washington Technology Solutions

2024 State Agency Privacy Assessment

April 1, 2025

Office of Privacy and Data Protection

Table of contents

Introduction

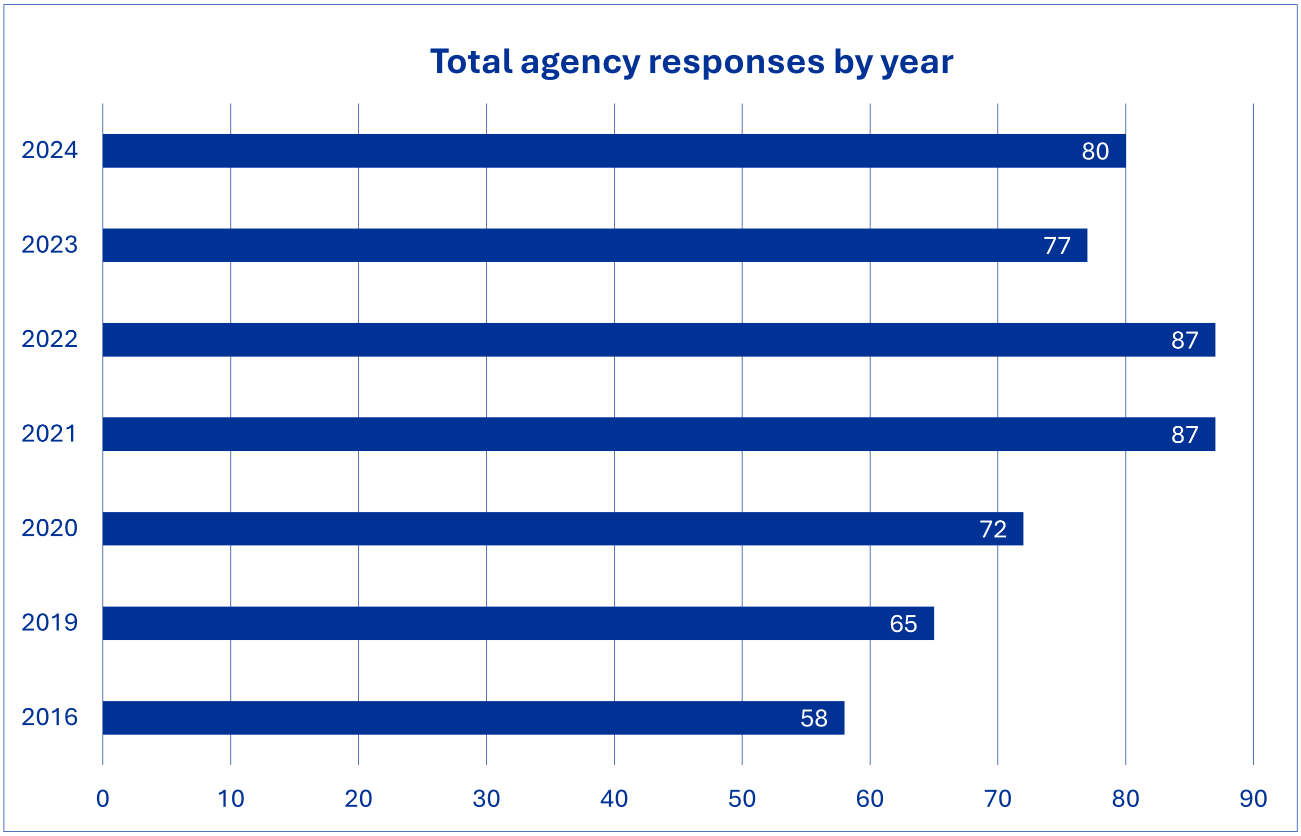
Consistent with past years, state agencies show continued improvement in the implementation of privacy protections, privacy awareness and privacy maturity.

RCW 43.105.369 requires the State Office of Privacy and Data Protection (OPDP) to conduct an annual privacy review of state agency privacy 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 a general assessment of privacy implementation across the state enterprise, and not an audit of specific agencies.

Results from the 2024 survey indicate agencies continue to improve in the implementation of privacy protections, awareness and maturity. OPDP believes this improvement is a result of agencies developing and maturing their privacy programs and increasing awareness, developing resources, cross-agency collaboration, and the combined support from both the Governor and Legislature. There has been consistent improvement over the past five years of the survey.

The 2024 assessment covers many basic components of a privacy program and aligns with the OPDP state Privacy Framework and the state Agency Privacy Principles. Washington was one of the first states in the nation to develop state specific privacy prinicples, a privacy framework and training. With the adoption of the enterprise wide Privacy and Data Protection Policy, Washington state continues towards more standardization across agencies.



There was a slight uptick in the number of state agencies responding to the assessment this year, 80 versus 77 in 2023. Of the 80 agencies that reponded this year, 70 hold personal data. While the legislative branch did not complete the survey for any of its agencies this year, more small agencies did respond. In the past, legislative branch agencies accounted for close to a dozen responses, despite the fact they are not required to submit the survey. Many small agencies combine their responses with larger support agencies which also accounts for some variance in responses year to year. Despite the variance in responses, the data offers an excellent insight into privacy work across state government.

Privacy maturity continues to improve across the enterprise, but continued 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 annual assessment to agencies as part of the 2024 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. In 2024, of the 80 respondents, 70 agencies indicated they collect and maintain some personal information. Data in this report is based on those 70 agencies. As a comparison: In 2021, 72 of 87 agencies indicated they collect and maintain personal data. In 2022, 74 of 87 agencies indicated they collect and maintain personal data and in 2023, 68 agencies of 77 indicated they collect and maintain personal data.

Personal information – also commonly referred to as personal data or personally identifiable information (PII) – is defined as information identifiable to a specific individual. Using the foundation of the state privacy principles, and state privacy framework, the 2024 Privacy Assessment Survey gathered information in several areas including:

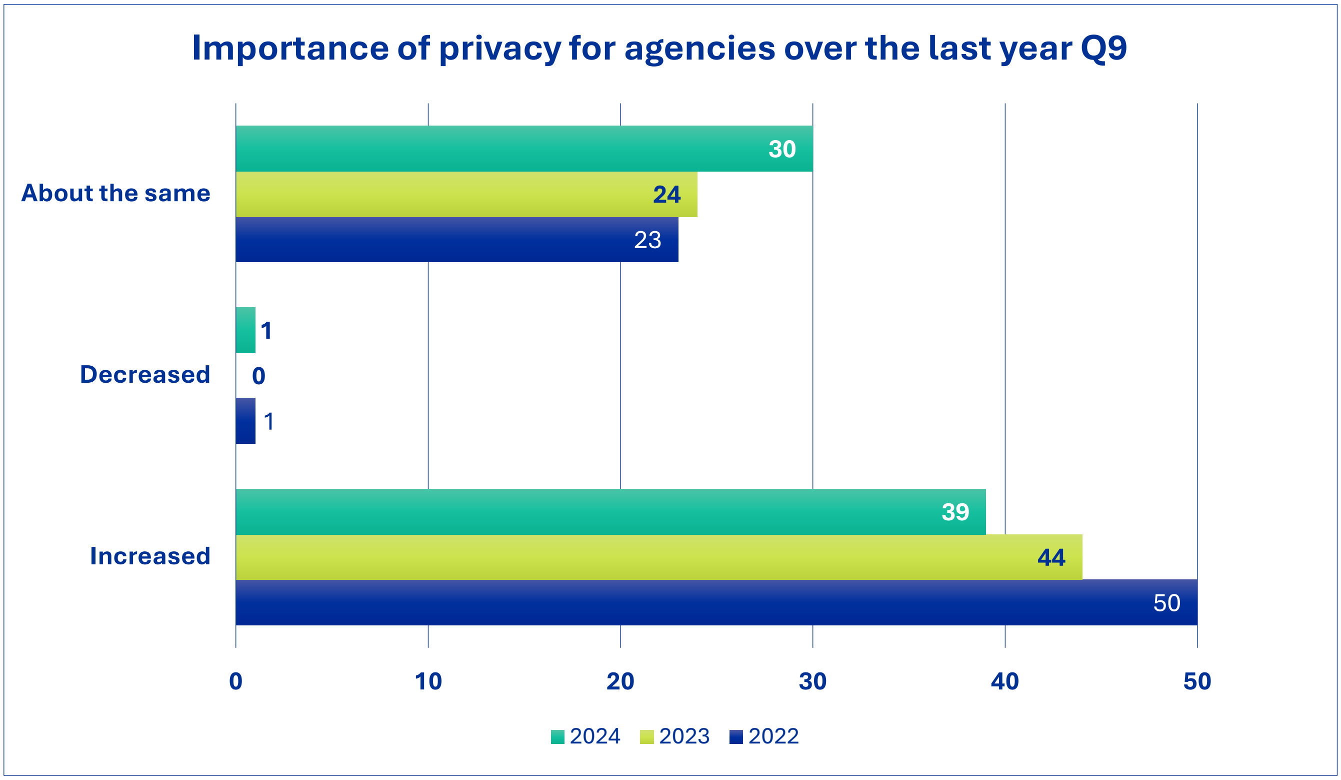
- Types of personal information.
- Privacy roles and staffing.
- Training and policies.
- Transparency.
- Individual participation.
- Metrics.
- Accountability.
- Data sharing.
- Data inventory.
- Future planning.

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, not individual agencies.

Many agencies in 2024 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 both 2022 and 2024, only one agency said privacy became less important.

Forty-one agencies reported privacy had become more of a priority this year. This year's measurement of the importance of privacy 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. More agencies this year report that privacy has remained about the same in importance. This is probably due to the recent efforts at increasing privacy maturity across the enterprise, as well as some agencies that have had privacy protections baked into their functioning (most notably, the health care, education, or financially focused agencies.)

A note about the charts in this report. The numbers in the charts represent agencies that answered the survey question at the top of the chart. Agencies that responded and do not maintain personal data are not represented in the charts. Each chart is labeled with the survey question number to make it easier to look up the data. For example, the chart below corresponds to question nine (Q9) and shows that in 2024 there were 39 agencies responding that privacy has become more important over the past year.

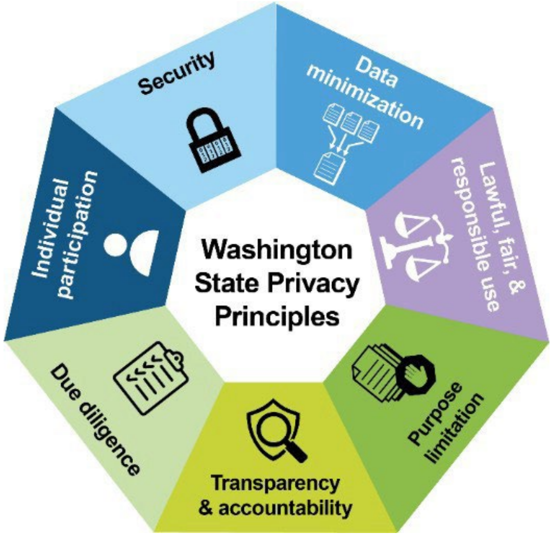


Overall, OPDP found that agencies are more likely to have core privacy program components – such as dedicated staff and formal policies and trainings than in the past. However, gaps remain and even agencies with more privacy experience consistently indicate they need additional resources. This need will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

As a foundation for privacy program development, the OPDP articulated the Washington State Agency Privacy Principles with the input and collaboration of state agencies. This report makes connections between the survey data and the state privacy principles throughout. These principles are often referenced as one of the many resources developed by the OPDP to assist on the maturity journey of state agencies.

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

In 2023, OPDP 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 illustrates that privacy maturity is an ongoing, continual improvement process. 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.


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

In 2024, OPDP developed a Privacy and Data Protection Policy for the whole state, as well as resources to help implement this newly adopted policy. The goal of the Privacy and Data Protection policy was to peel out privacy focused data management requirements from other policies, such as security, and make them easier to understand and implement across the enterprise.

Types of Personal Information

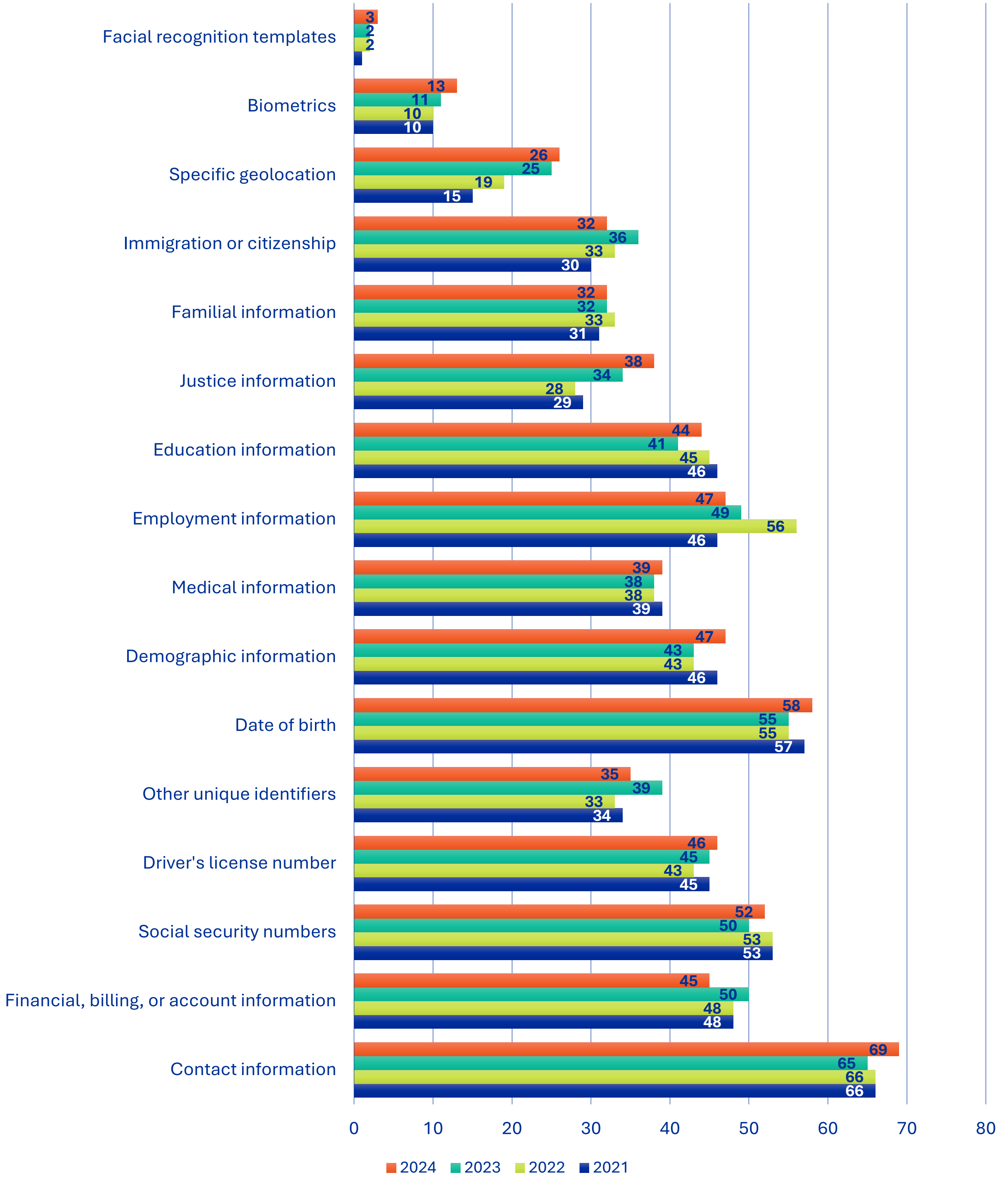
The privacy assessment gathered information from agencies about the types of personal information they maintain and the sources of that information. The assessment revealed that many agencies maintain diverse types of sensitive personal information based on their mission and focus.

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.

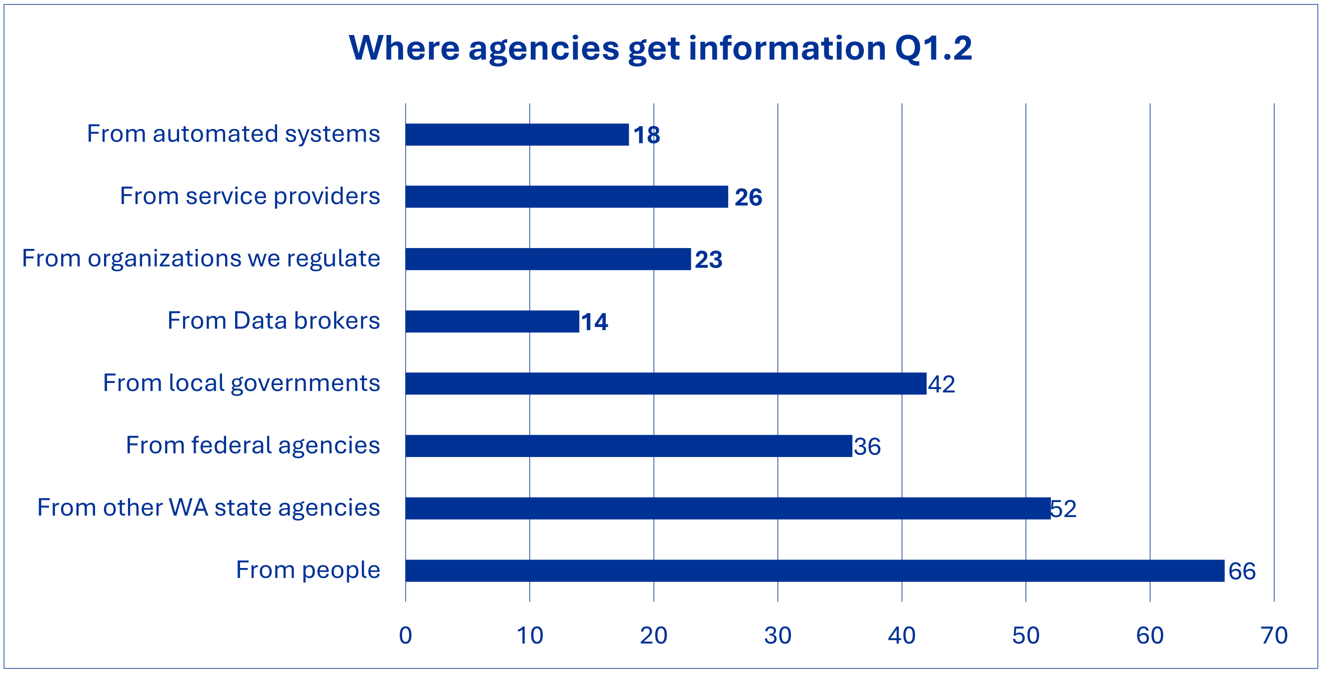
The type of information agencies maintain is important as a determination for the type of privacy controls needed to minimize risk and appropriately protect the information.

The types of information that agencies maintain varies widely. In 2024, contact information is the most common type of information held by agencies (69 agencies).

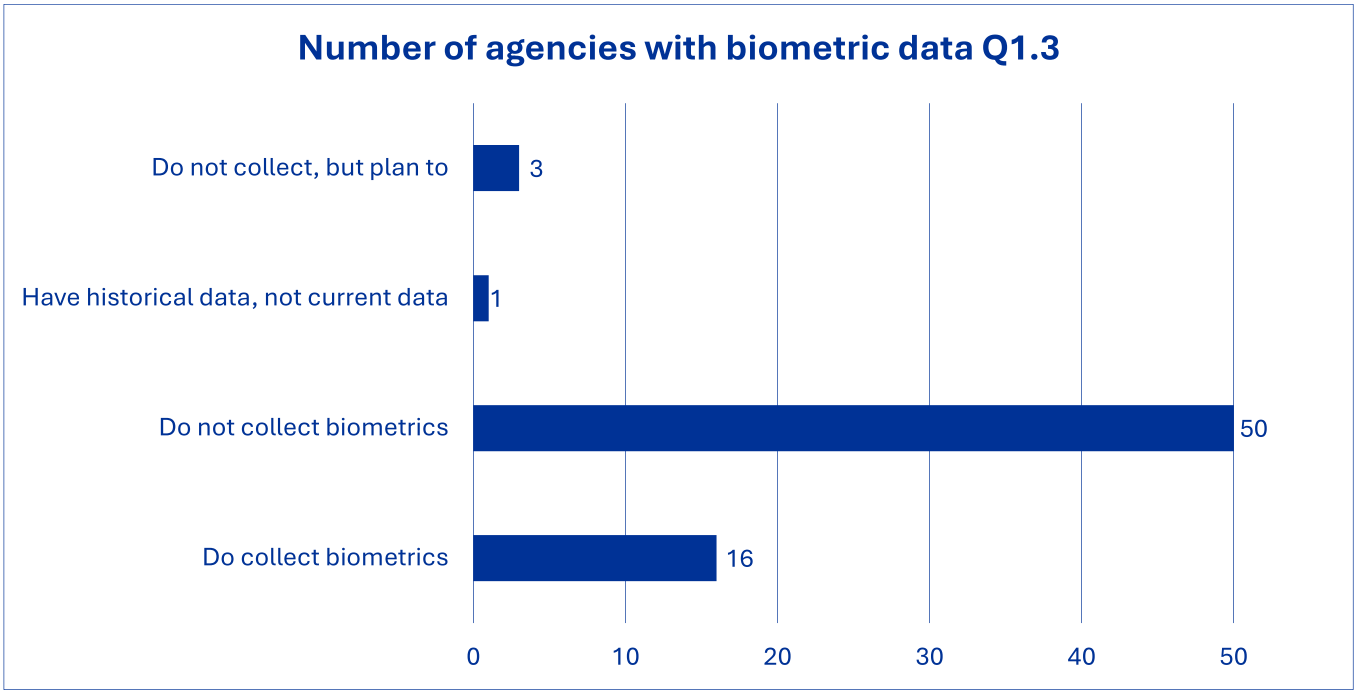
Types of data held by agencies Q1.1



The next question in the survey asked where agencies get the data they hold. Sixty-six agencies reported they get the data from people (to provide services, or as required by law.) Only 18 agencies reported they receive data from automated systems, and 52 agencies get their data from other Washington state government agencies.



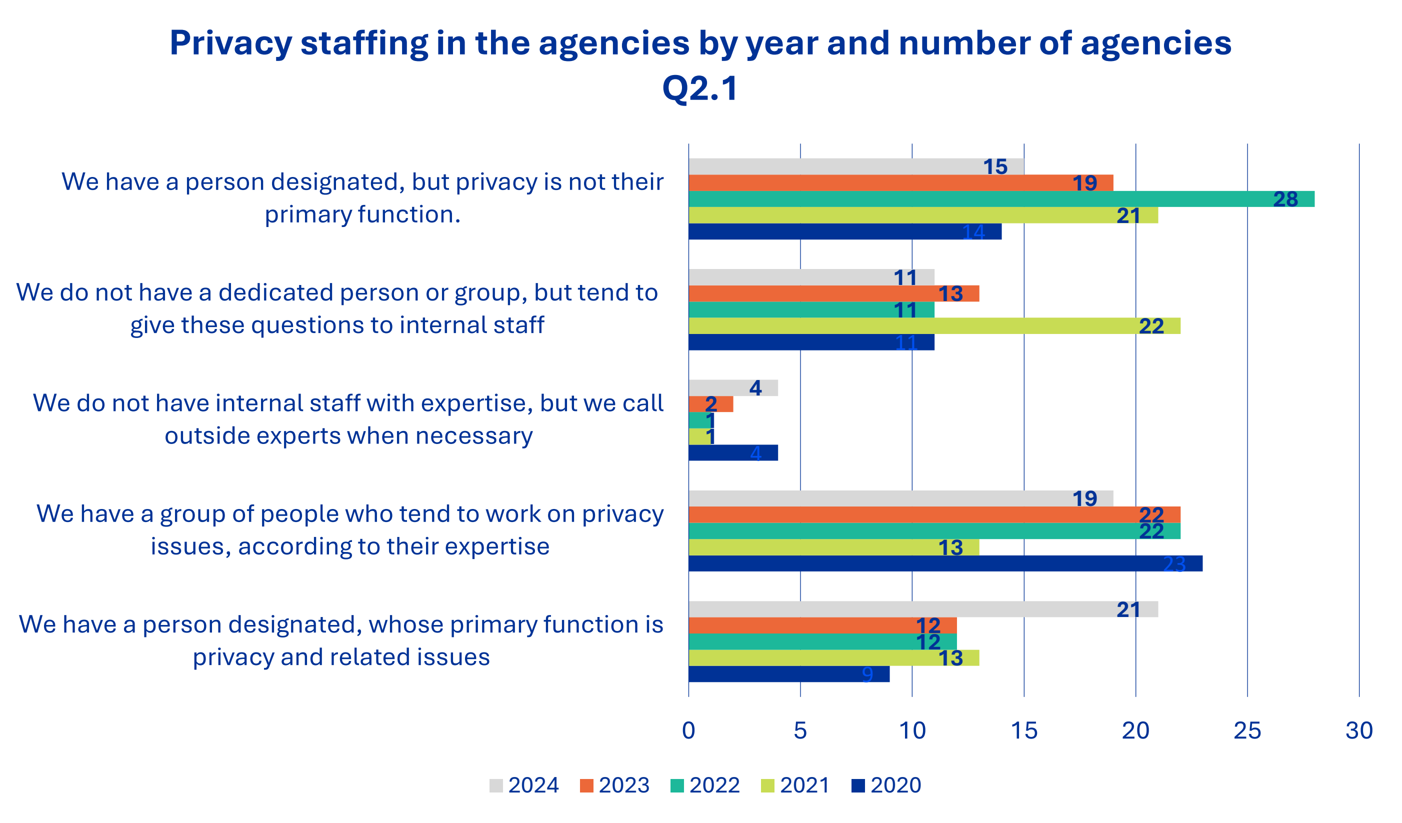
Over the last few years, there has been an increasing interest in the policies around biometric data. In Washington state 50 agencies reported they do not collect any biometrics. Sixteen agencies reported they do collect biometric data, and three agencies are currently in the process of developing standards 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 current 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 2024, 37 (up from 31 agencies in 2023) said they have a specific person designated to handle privacy policy issues (either as a primary or secondary responsibility).


Privacy staffing in the agencies by year and number of agencies Q2.1

The number of agencies reporting no one tasked with privacy policy is a positive metric for the enterprise. OPDP feels this low number is due to better awareness of privacy issues, the newly adopted enterprise privacy policy, and the robust availability of privacy related training and resources. 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. OPDP strives to support all of these individuals across state government.

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.

OPDP has developed and implemented training for state agencies that can be utilized by personnel in any discipline – so that privacy protections can be enhanced. Dedicated staffing within agencies allows the OPDP to better target assistance for customer agencies with privacy work, training, or program development.

An example of OPDP support for privacy development at agencies is the convening of the community of practice for privacy professionals at the state level. This group is modeled on other existing communities of practice drawn from across agencies and has developed 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. OPDP has also pursued and received federal grant funding to increase the number of certified privacy professionals at the state and local level.

Agency Privacy Policies

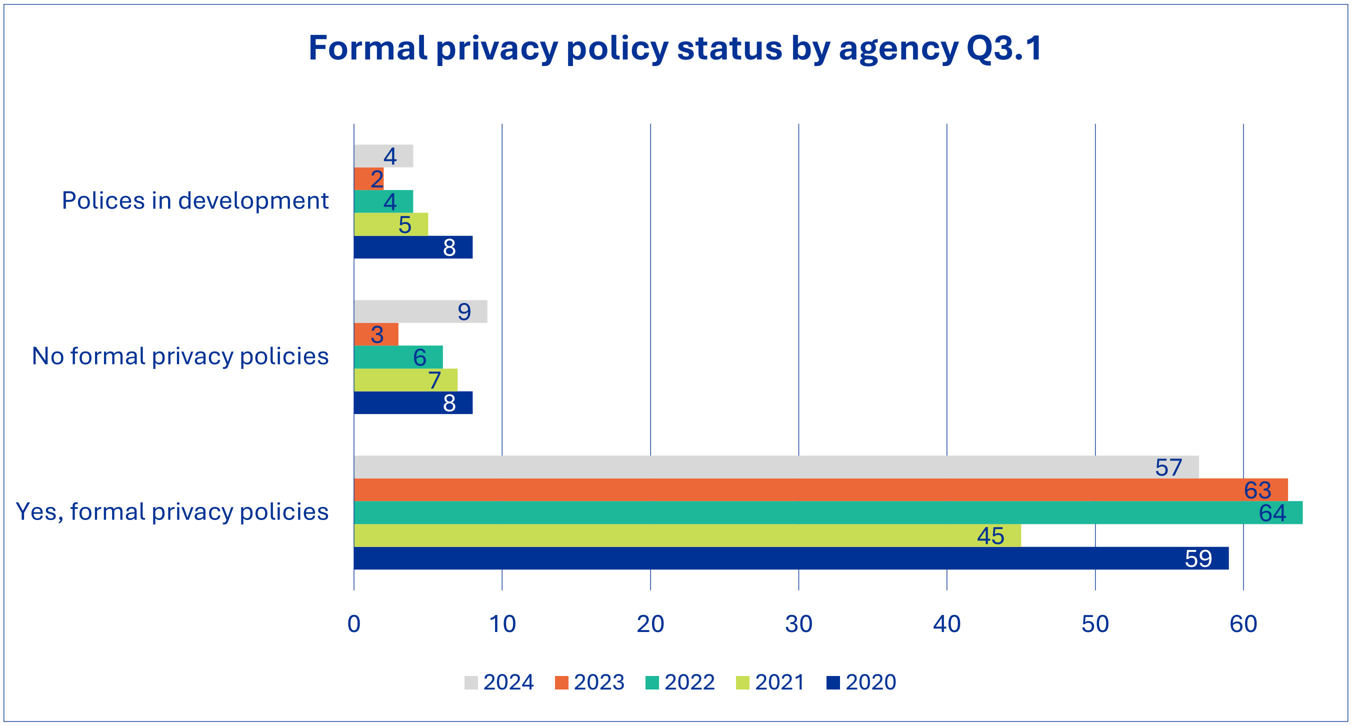
Most state agencies that maintain personal data have started the process of implementing the concepts in the Washington State Privacy Principles and the Washington State Privacy Framework for agency data protection.

Internal agency privacy policies apply to how information is collected, used and shared. Policies 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.

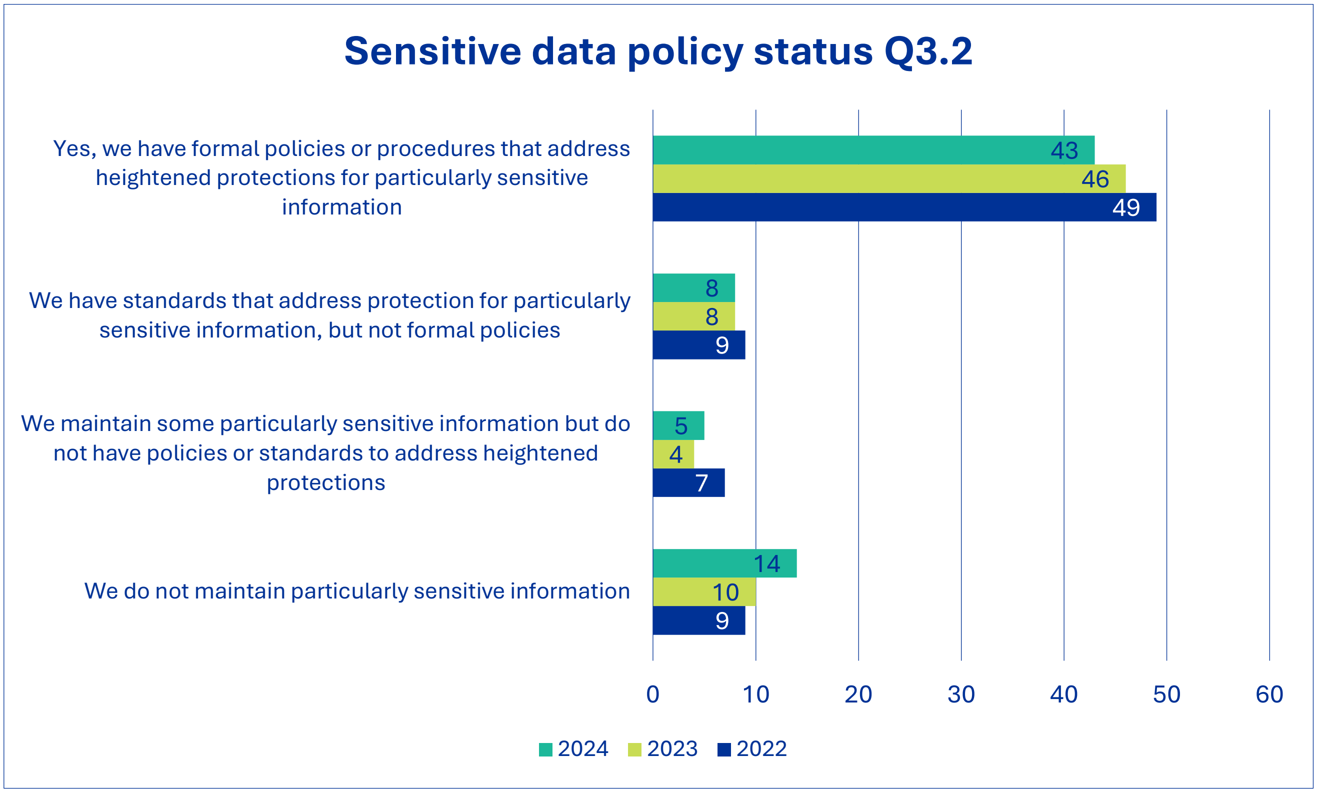
There appear to be two factors driving adoption and implementation of formal privacy policies:

1. The newly adopted enterprise privacy and data policy.
2. Greater awareness and importance of privacy.

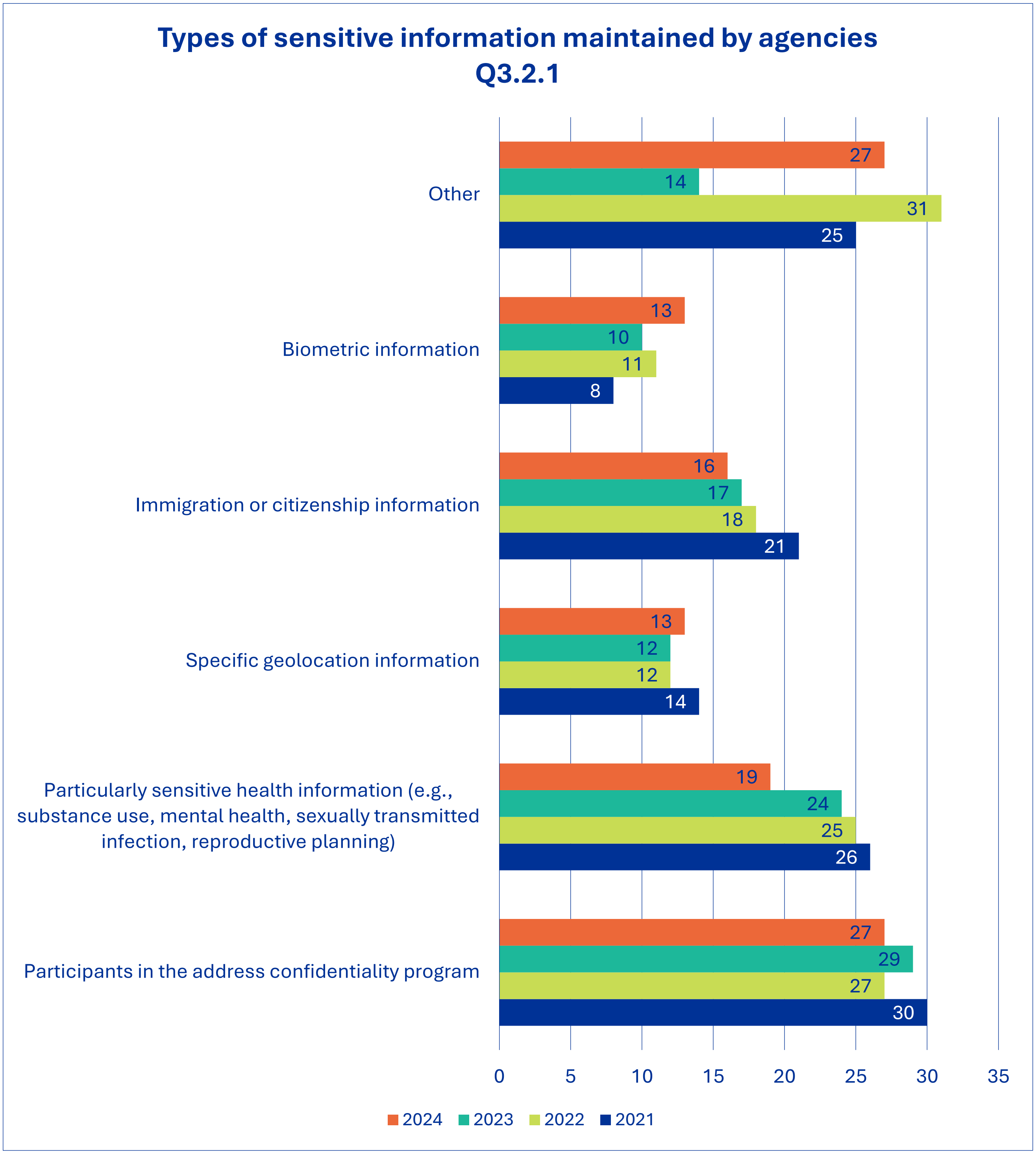
Both factors have resulted in more policy development. Support from legislative and executive branch leadership has also been crucial.



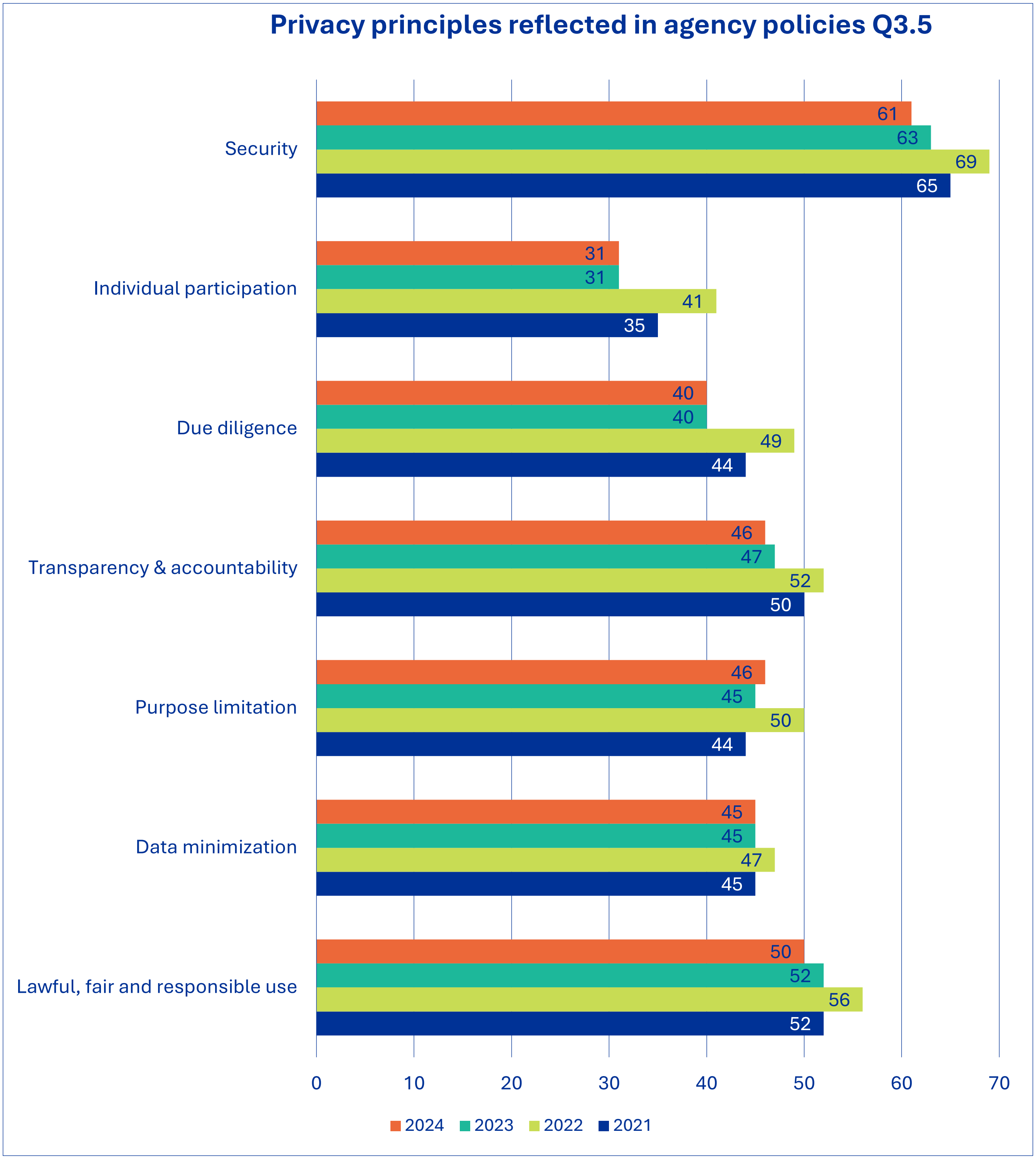
Within the general scope of privacy policies, the survey asked about specific policies around particularly sensitive information. The chart for question 3.2 shows agencies with formal policies, procedures, or other standards, that address heightened protections for particularly sensitive subsets of information. The responses between 2024, 2023, and 2022 are consistent.



The survey drilled deeper into the exact kinds of data that are protected by policy, procedures or standards. They include: information from the state address confidentiality program, health information (substance use, or mental health data), specific geolocation information, immigration or citizenship information, and biometric information.



The state privacy principles guide specific privacy policies within state agencies. Year over year comparisons are consistent across the privacy principles reflected in agency policy. The "Security" privacy principle is the one most often reflected in 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 organization 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 protections. 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.

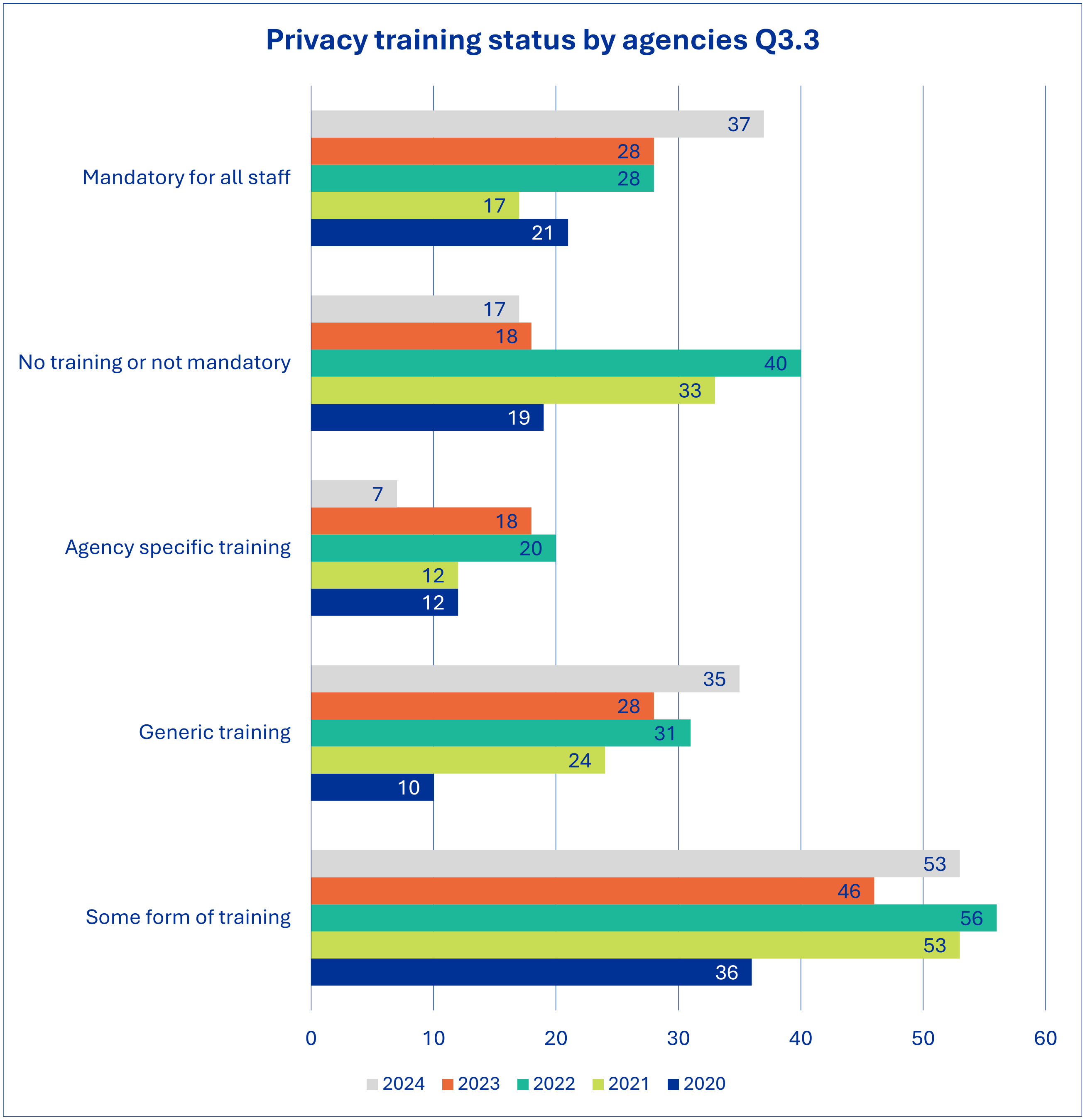
OPDP developed statewide training to help agencies build awareness of the importance of privacy. This Privacy Basics training for Washington state employees is available to all state agencies through the enterprise learning center or via the OPDP website. The training is also being piloted to local governments that are interested in using it in whole or in part.

In addition to 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 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 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 2024 responses indicate a majority of 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 part of cybersecurity training. Standalone privacy training (either generic or specific) is beneficial for a better awareness and application of agency privacy policies.



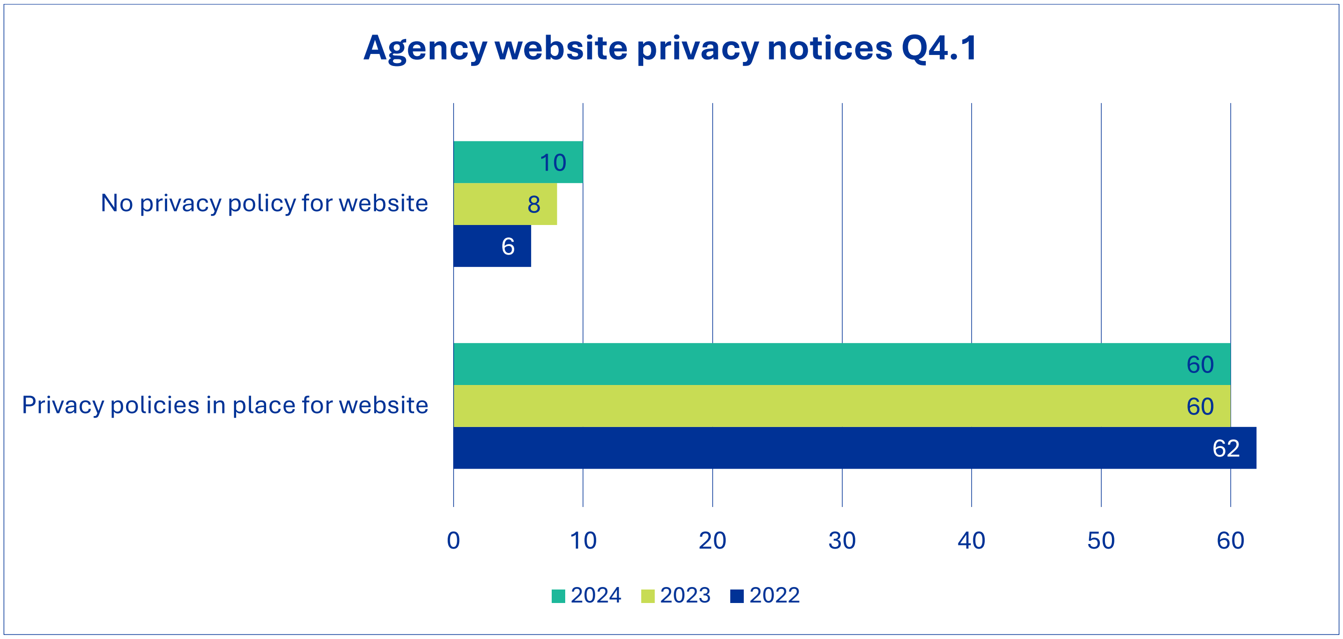
Of the 53 agencies that offer training, 35 agencies reported generic privacy training, and seven reported agency-specific training. (Eleven agencies did not indicate if the training they offer is generic or agency-specific). More agencies require privacy training now than in the past. More agencies are also making privacy training mandatory for employees.

OPDP reported last year that this was an area to watch as the state-specific OPDP developed privacy training was adopted across the enterprise. Expectations of more employees trained were met as agencies utilized the OPDP training. The OPDP prioritized creating a statewide privacy training program based on information from past surveys. Details of OPDP training utilization can be found in the OPDP four year performance report that can be found here: OPDP Performance Report 2024

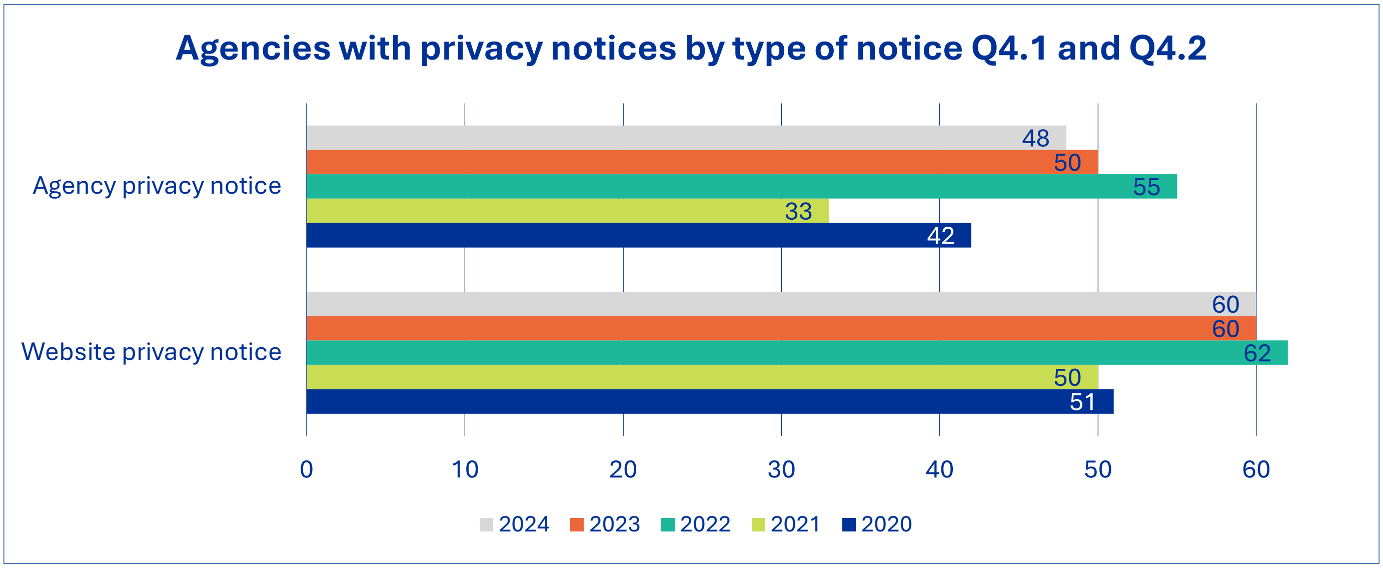
Transparency

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.

To target transparency, agencies were asked about their 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. Agencies collect personal information in a variety of ways, including from online portals, paper forms, in-person, other agencies, or through third parties. In 2024, 60 agencies indicated they had a website privacy policy.



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. Website privacy notices and agency privacy notices were measured as two distinct policies for explaining agency data collection and use. Expansion of privacy policies by agencies is clear in the reponses.

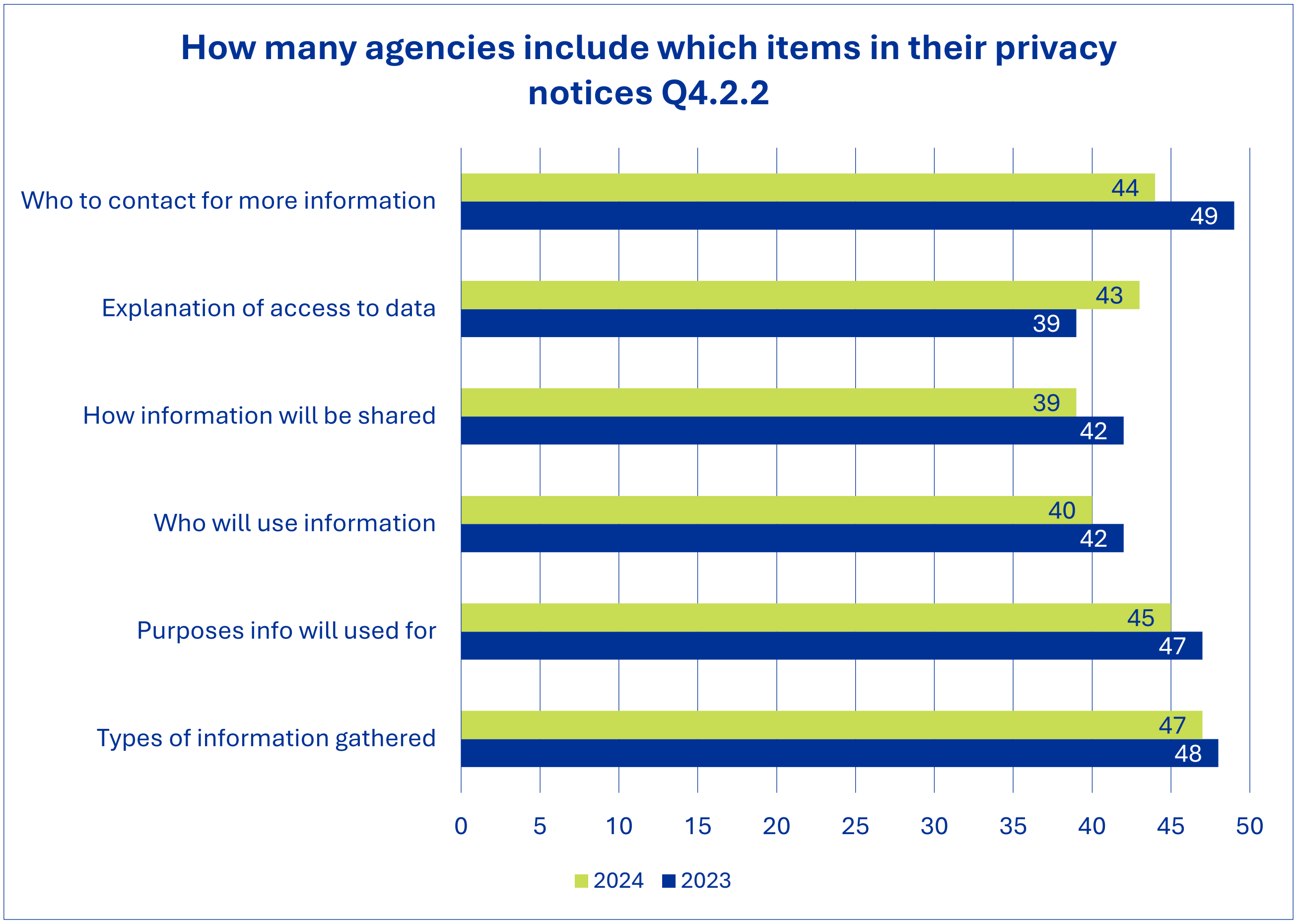


More than half of the agencies with personal information (48 agencies), indicated they have this type of comprehensive privacy notice. Most agencies post it on their website, while some also mail the notice or provide it in-person. This continues to be an opportunity for improvement, as many of these 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.



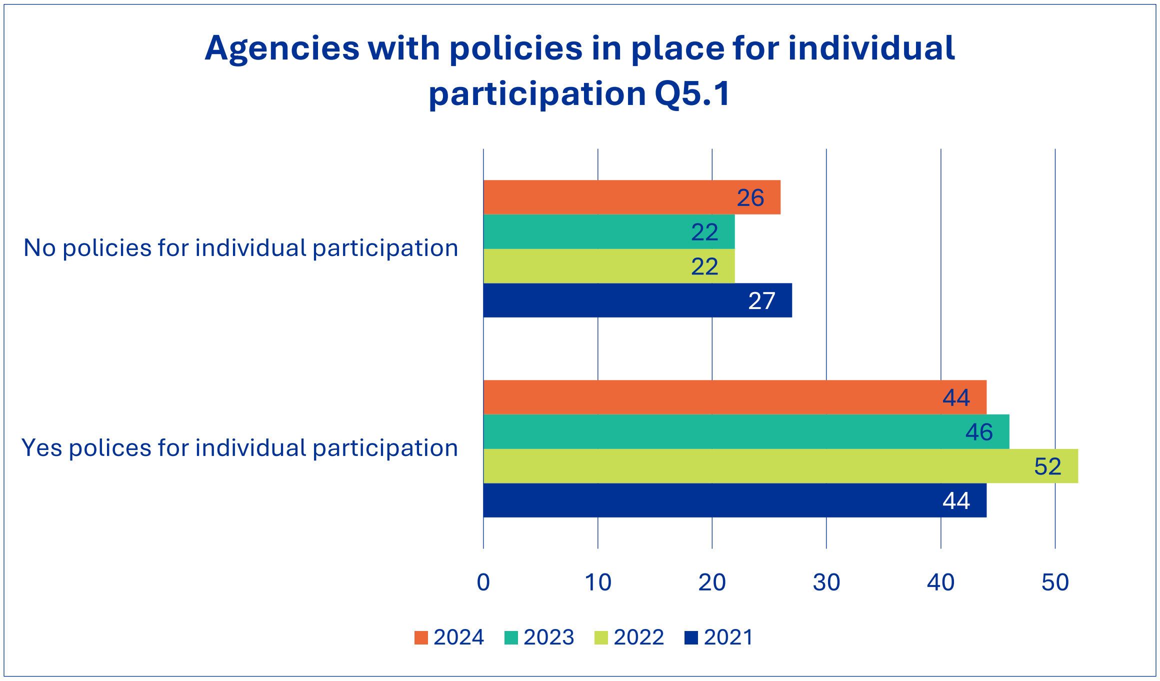
Individual Participation

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

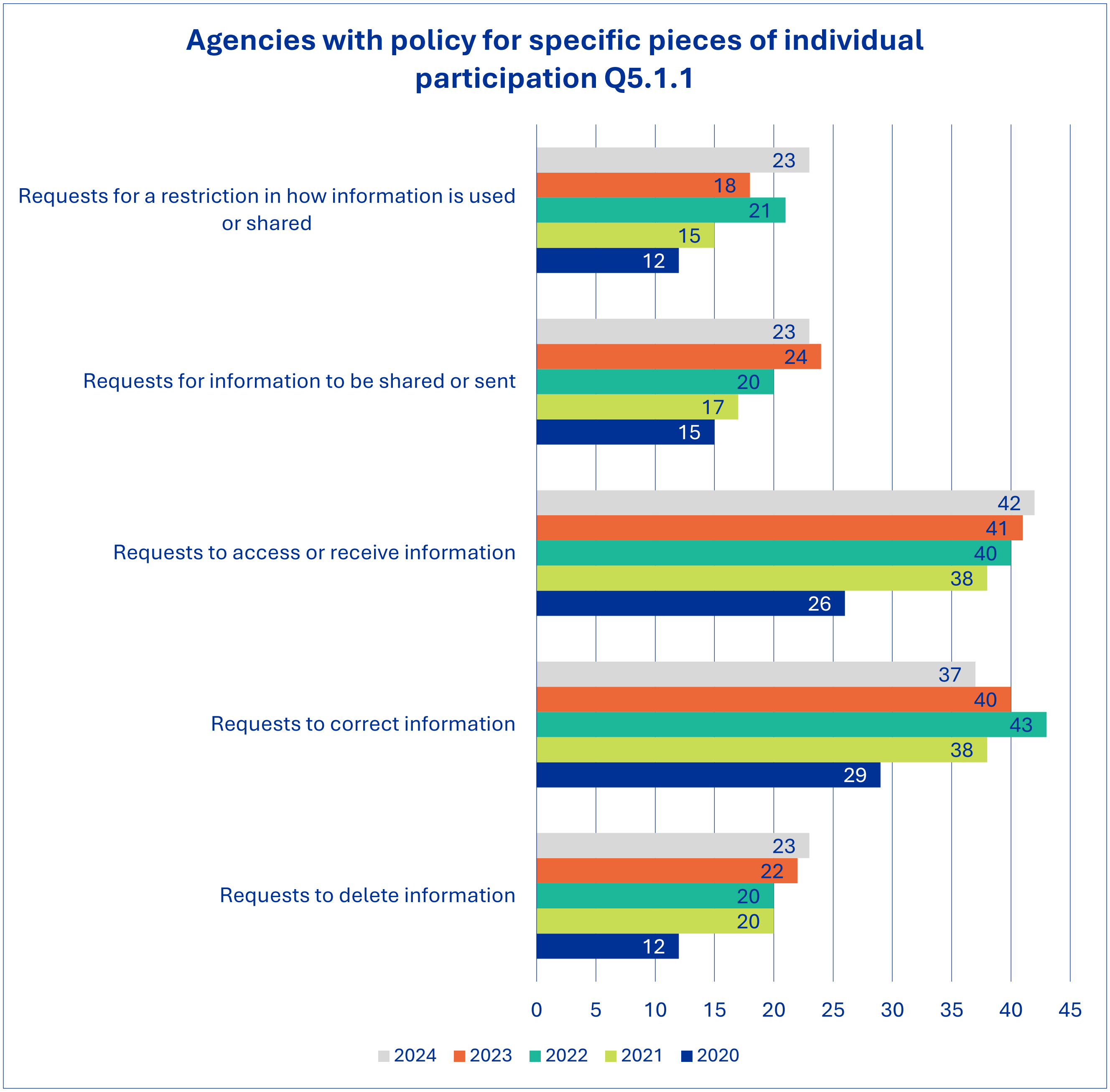
- To access or receive information.
- To correct information.
- To delete information.
- For information to be shared or sent to another person.
- For a restriction in how information is used or shared.

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 in 2024 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-eight agencies reported they have at least one, (46 in 2023, 52 in 2022 and 44 in 2021). Twenty-two agencie reported they do not have any procedures for individuals to control their personal data.



The next question in the survey drilled down into those agencies that had individual participation policies, and what those policies addressed. 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 (RCW 42.56).



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.

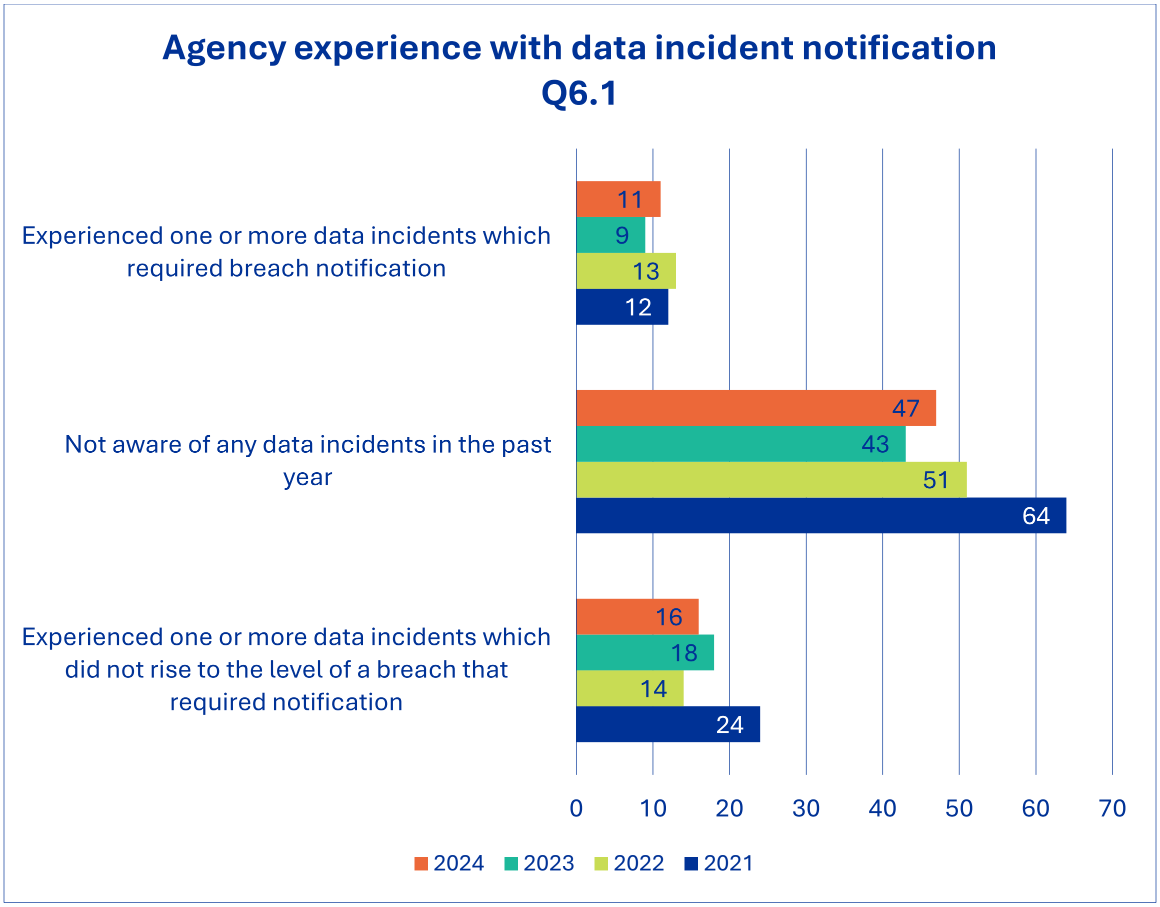
Agencies were asked about privacy incidents or breaches that occurred in the last year.

- 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 could be as simple as mailing information to the wrong person or disclosing information to an unauthorized person during a phone call.

The results from the 2024 assessment continue in line with past surveys.

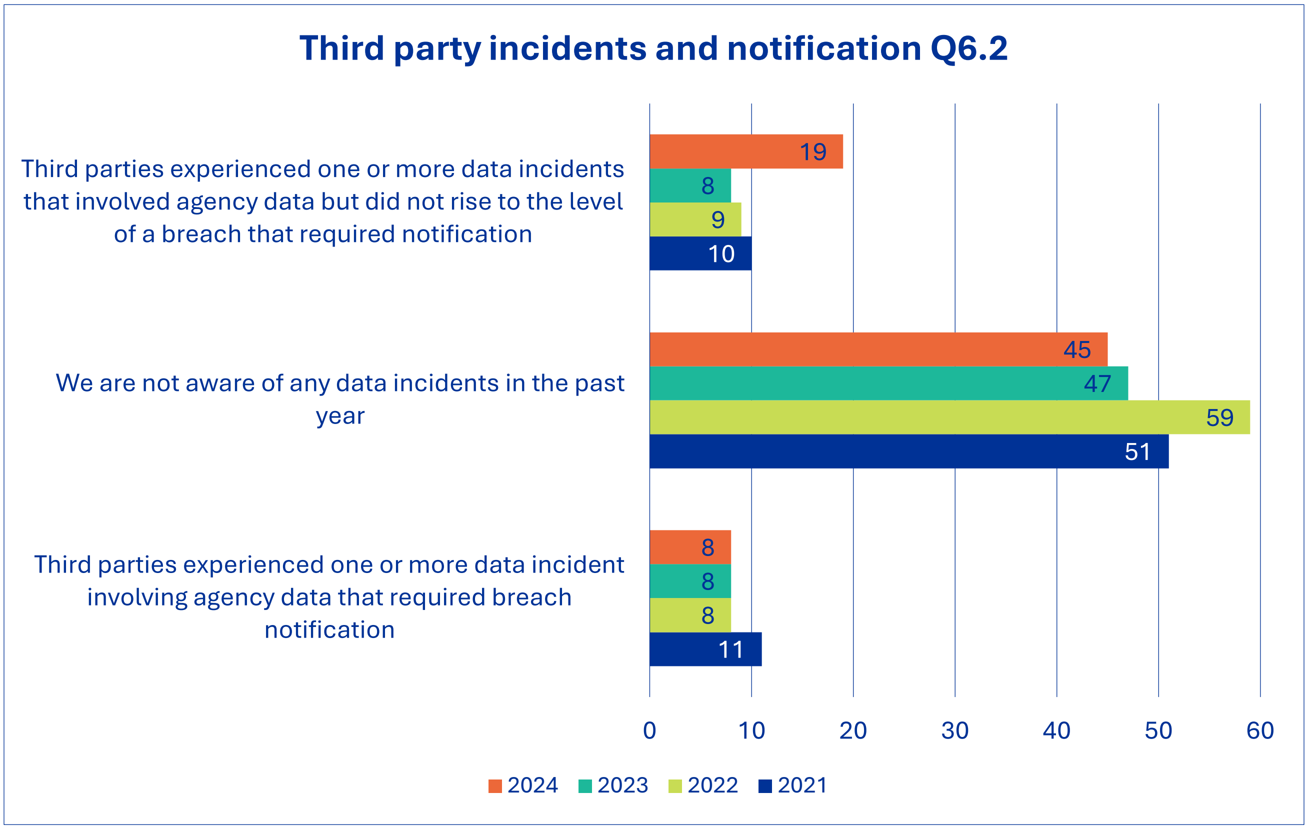
Detecting and responding to incidents is an indicator that appropriate controls are in place and staff understand how to identify and report them when there is unauthorized use or disclosure. When a state agency experiences no incidents, it could be a sign of excellent data protection and handling. It could also mean that incidents are going undetected due to inadequate controls.



In 2024 eleven agencies – not third parties – reported incidents that required breach notifications, 16 agencies had incidents that did not require notification, and 47 agencies reported they are not aware of any data incidents over the past year.

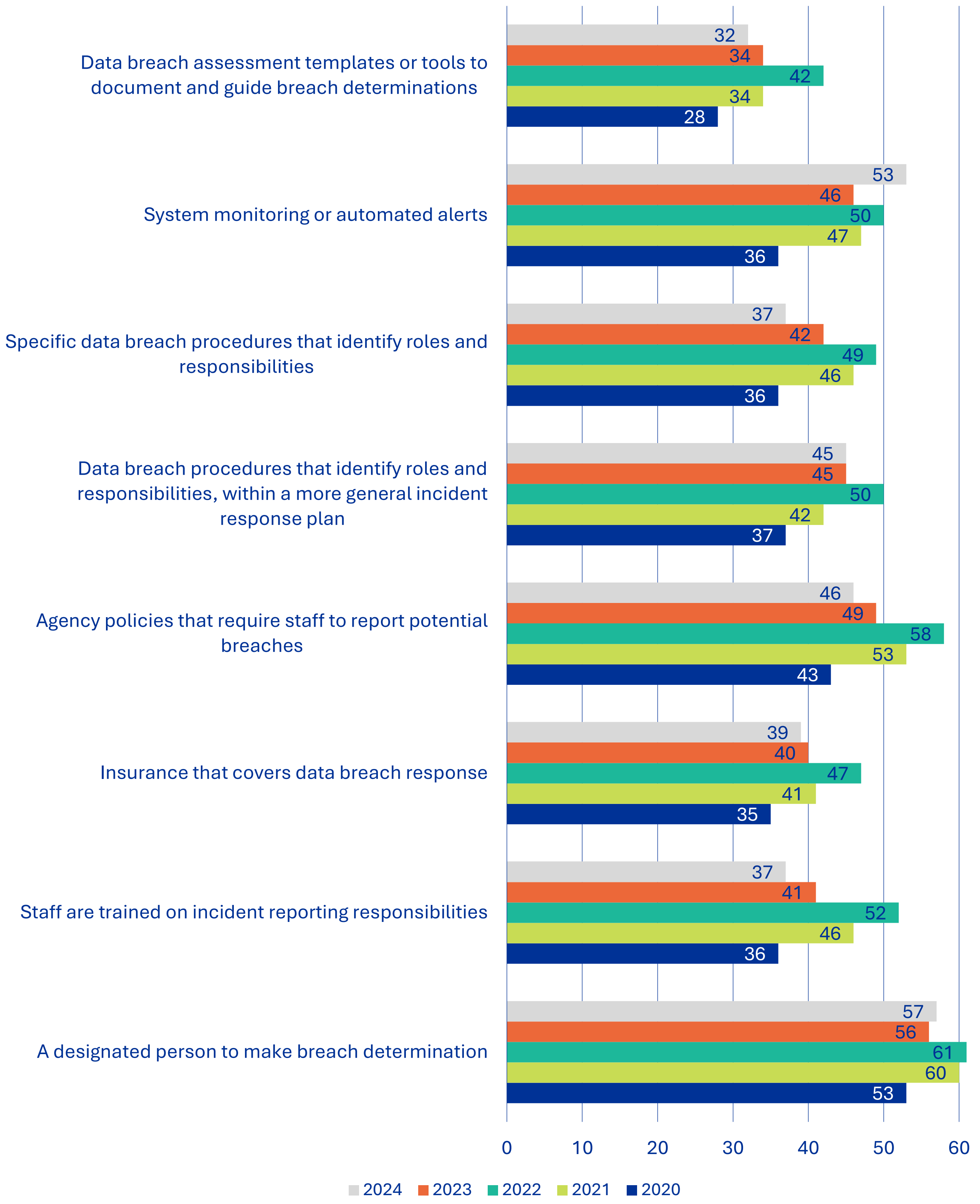
OPDP has expanded assistance to agencies through a Data Breach Assessment Form to determine if an incident has occurred and possible next steps.

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, agencies should also ensure third parties appropriately protect the information. Data sharing agreements (required though state policy and law) appear to have helped strengthen the tracking of vendors and data management.



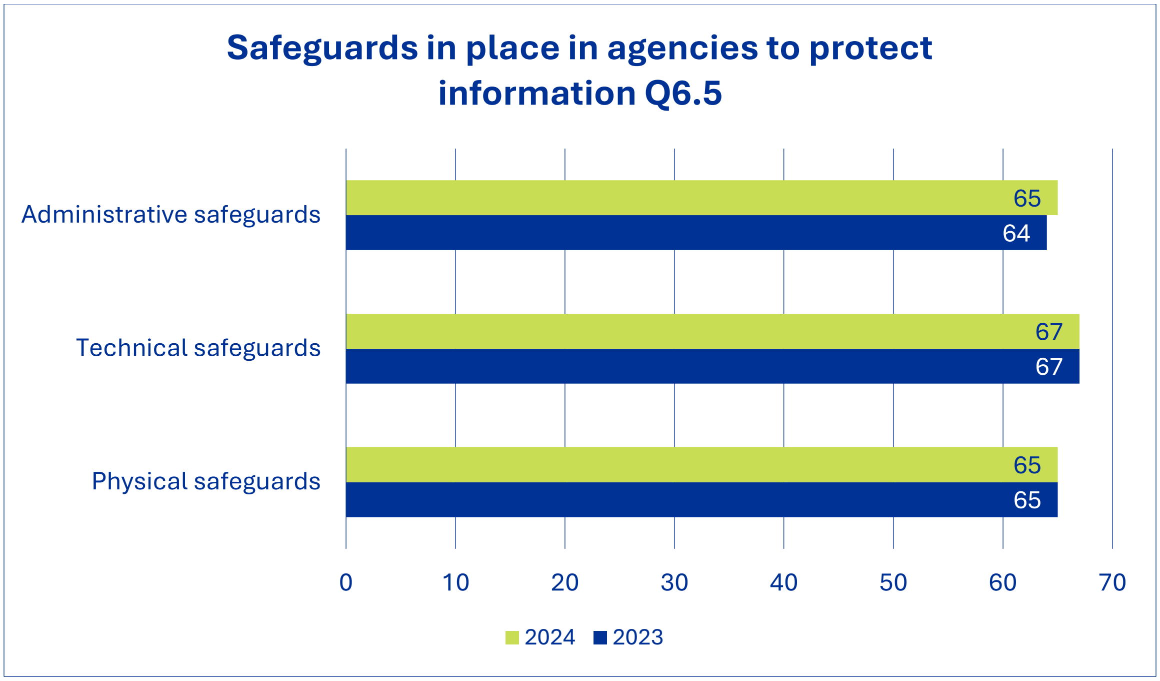
In 2024, 45 agencies were not aware of any third-party breaches, 19 agencies knew of data breaches which did not require notification, and eight breaches were known to require notification.

Agency controls for data breaches Q6.3



We asked agencies what steps they have taken to ensure incidents are discovered. Fifty-seven agencies have designated at least one person to make breach determinations. About half of those agencies have also implemented assessment tools or templates to address possible breaches. Overall agencies are improving in how they deal with data breaches and incidents.

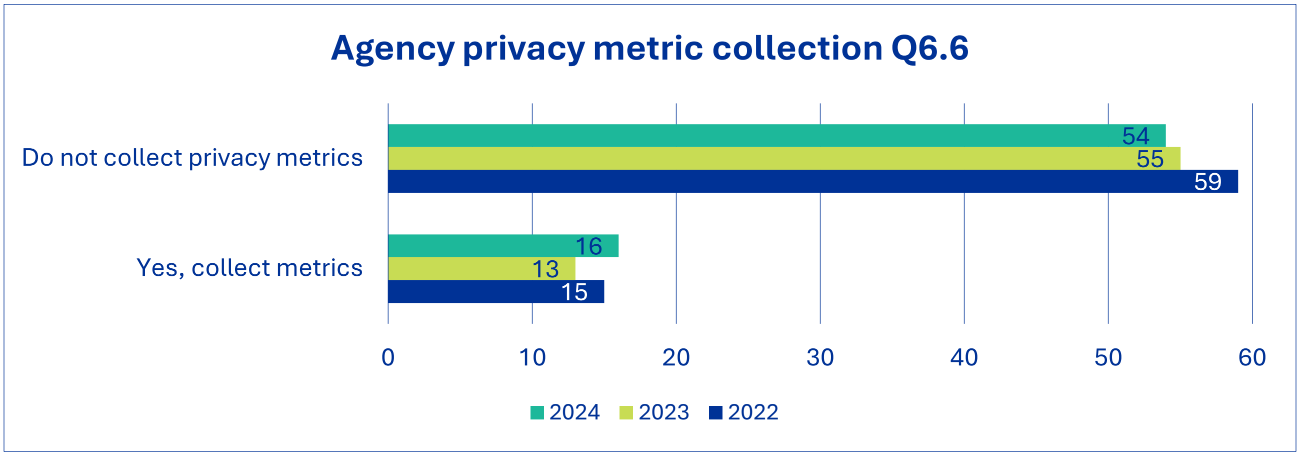
Focusing on specific kinds of controls for data protection the general assessment is positive across the state enterprise. Of 70 agencies responding to the survey this year, 65 have administrative safeguards in place, 67 have technical safeguards in place, and 65 have physical safeguards in place.



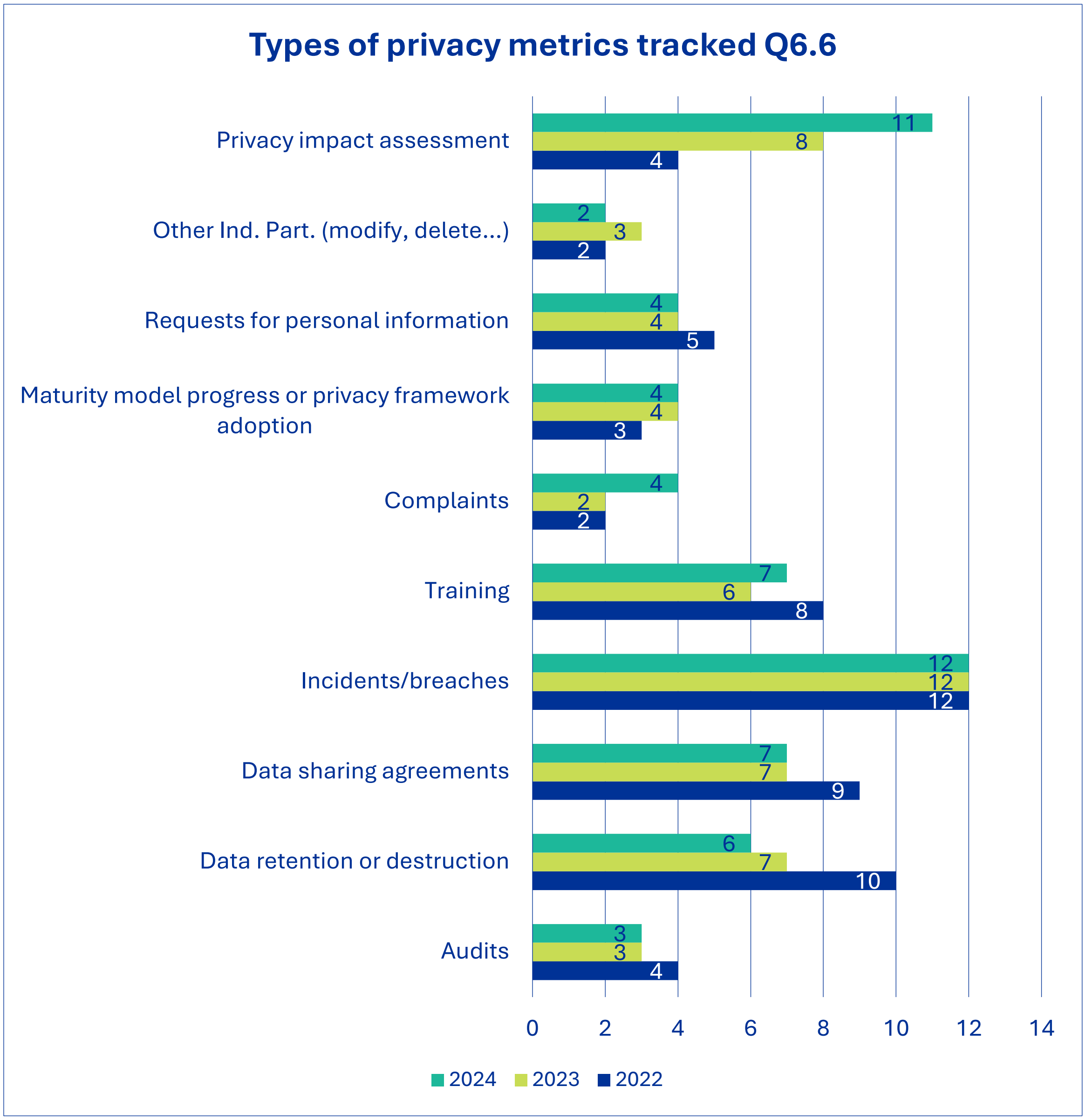
Measuring Privacy

New questions were added to the survey about measuring data privacy. OPDP is continuously working to find better ways to measure the maturity of privacy programs beyond this annual survey. To support this effort, the OPDP hosted a webinar on privacy metrics, and is watching the responses to this question in the annual survey.

Metrics can help clarify areas of excellence (or areas that need improvement) for individual agency privacy programs and illustrate progress within the State Privacy Framework. Metrics can be tailored to individual policies and data and can show opportunities for future progress. Only 16 agencies reported they collect metrics about their privacy programs.



Agencies that do collect metrics were asked about those metrics.



Data Sharing, Third Party Management, and Data Publishing

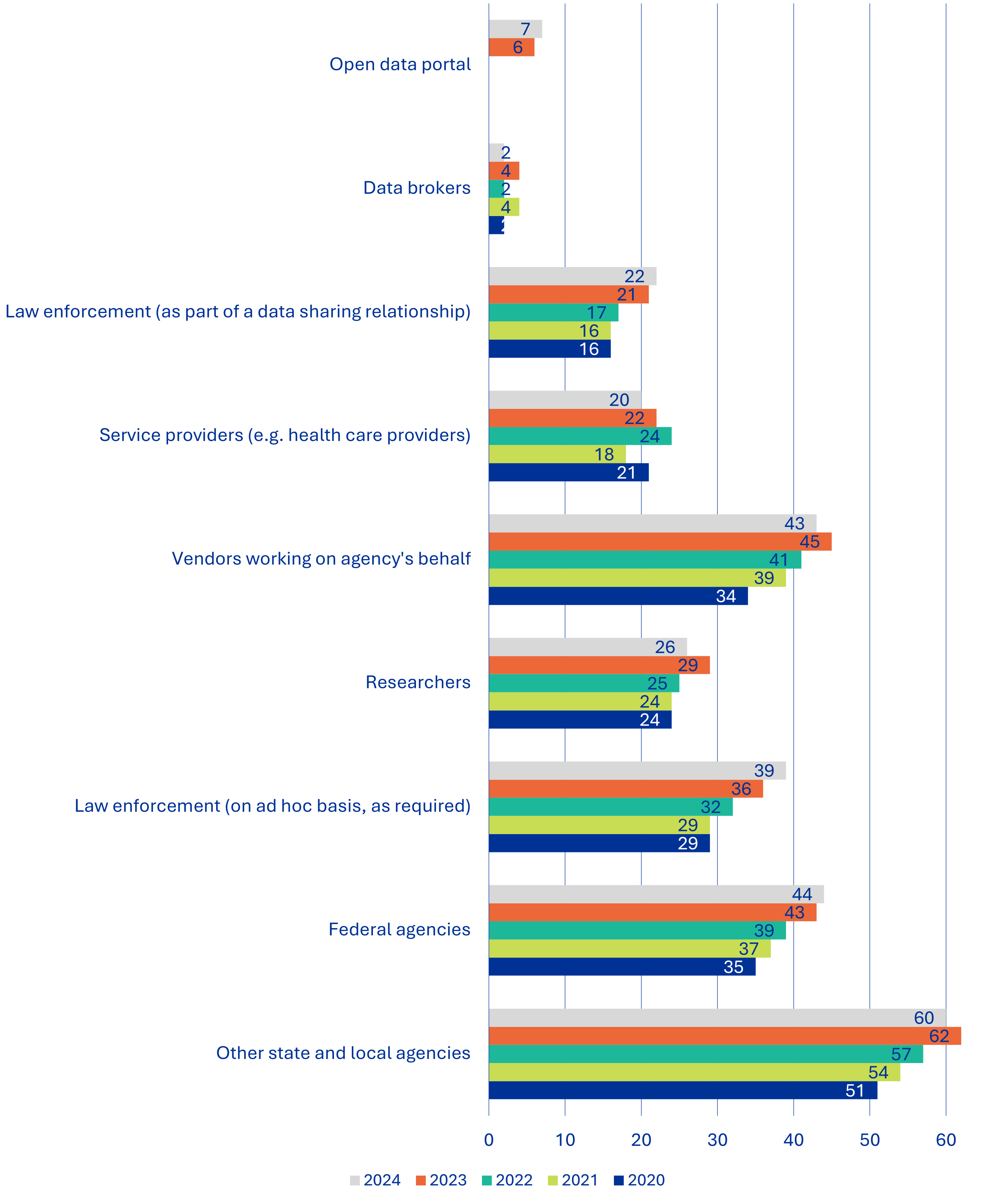
In today's data-driven world, information is shared in a variety of ways including between state agencies, with federal agencies, researchers, requests from law enforcement and when providing necessary access to a range of vendors and contractors.

An obvious question in this context is, "who are you sharing data with?" In 2022, more than 75% of agencies reported sharing personal information with other state or local agencies. In 2024 that number is up to more than 80% of reporting agencies sharing personal information with other state or local agencies.

Five years of consistent data illustrates the trend of more data sharing, not less. Legislation requires data sharing agreements for state agencies that share information, and the OPDP has helped create model terms for those data sharing agreements for state agencies as well as guidance.

A new category of data sharing was added to the survey in 2023 after discussions with agencies. The "open data portal" was added because six agencies reported sharing with an open data portal to provide better public access to data. That number is up to seven this year.

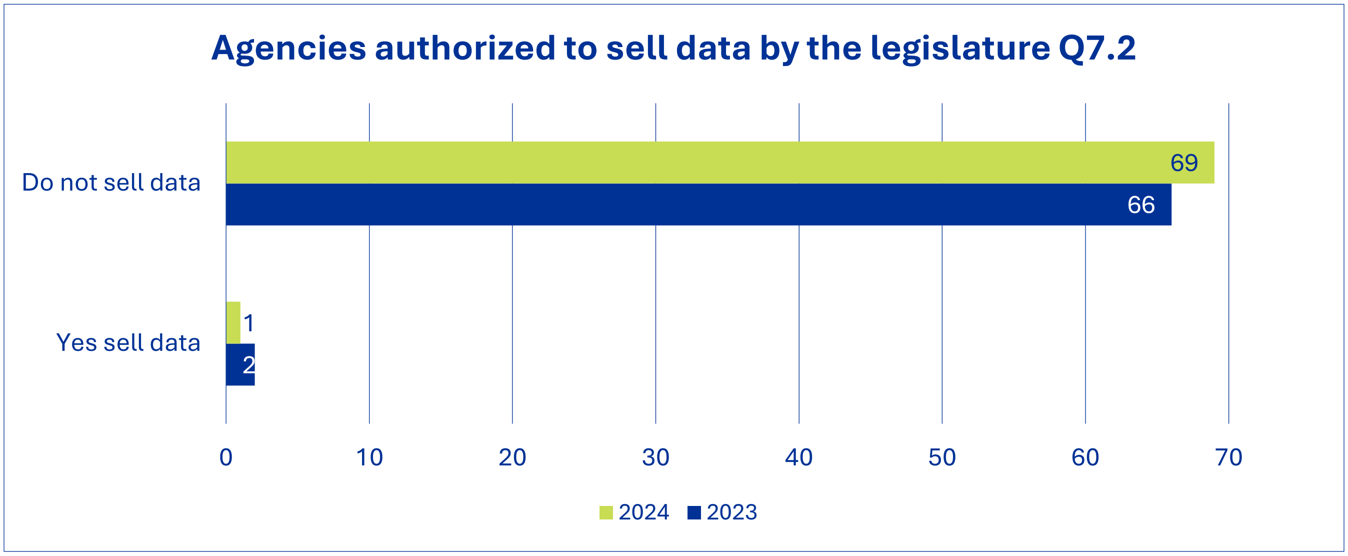
Who agencies share data with: Q7.1



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.

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. Agencies may view the Data Sharing Implementation Guidance developed by the 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 one state agency sells personal information. This is consistent with past surveys, and the agency cited the authority to sell data granted to them by the Legislature.



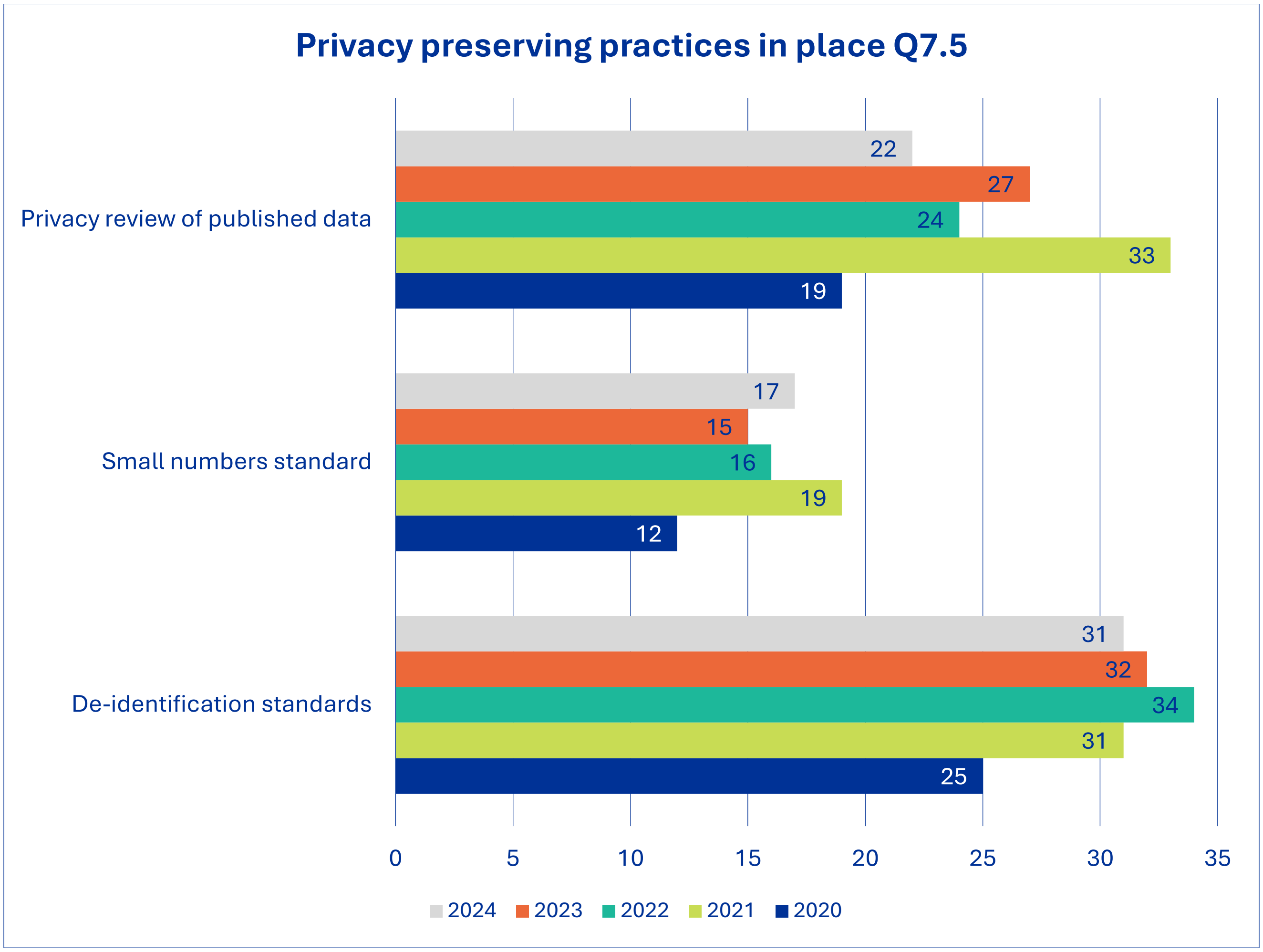
In addition to sharing personal information, agencies disclose information to remain transparent and accountable for government operations. These disclosures could include reports to the Legislature, publishing data on websites or open data portals, and sharing analysis with stakeholders. Agencies can 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.

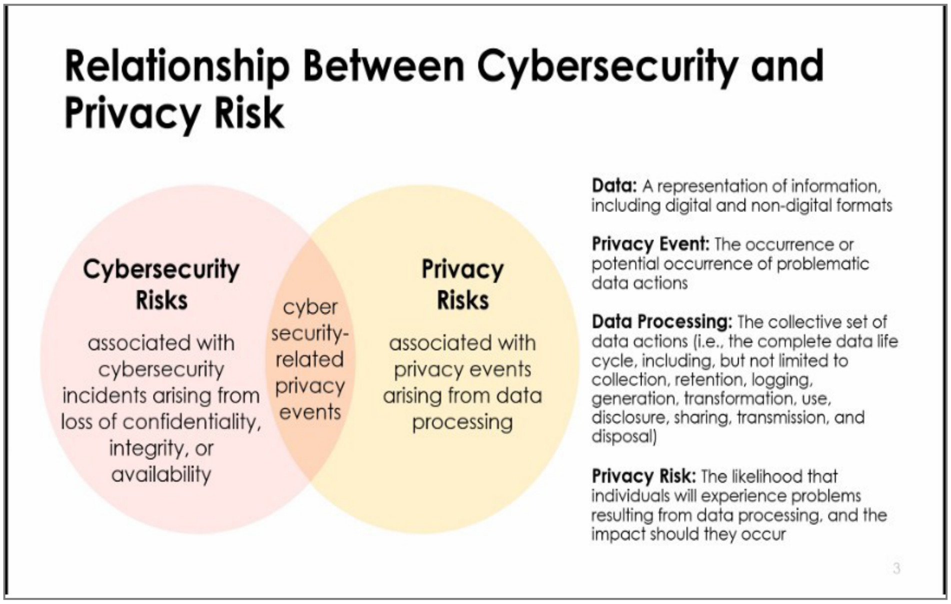
Dozens of agencies reported having these privacy-preserving practices in place for publishing public data.



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 (at right) also demonstrates the relationship between cybersecurity and privacy for data related events due to data processing activities.



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)

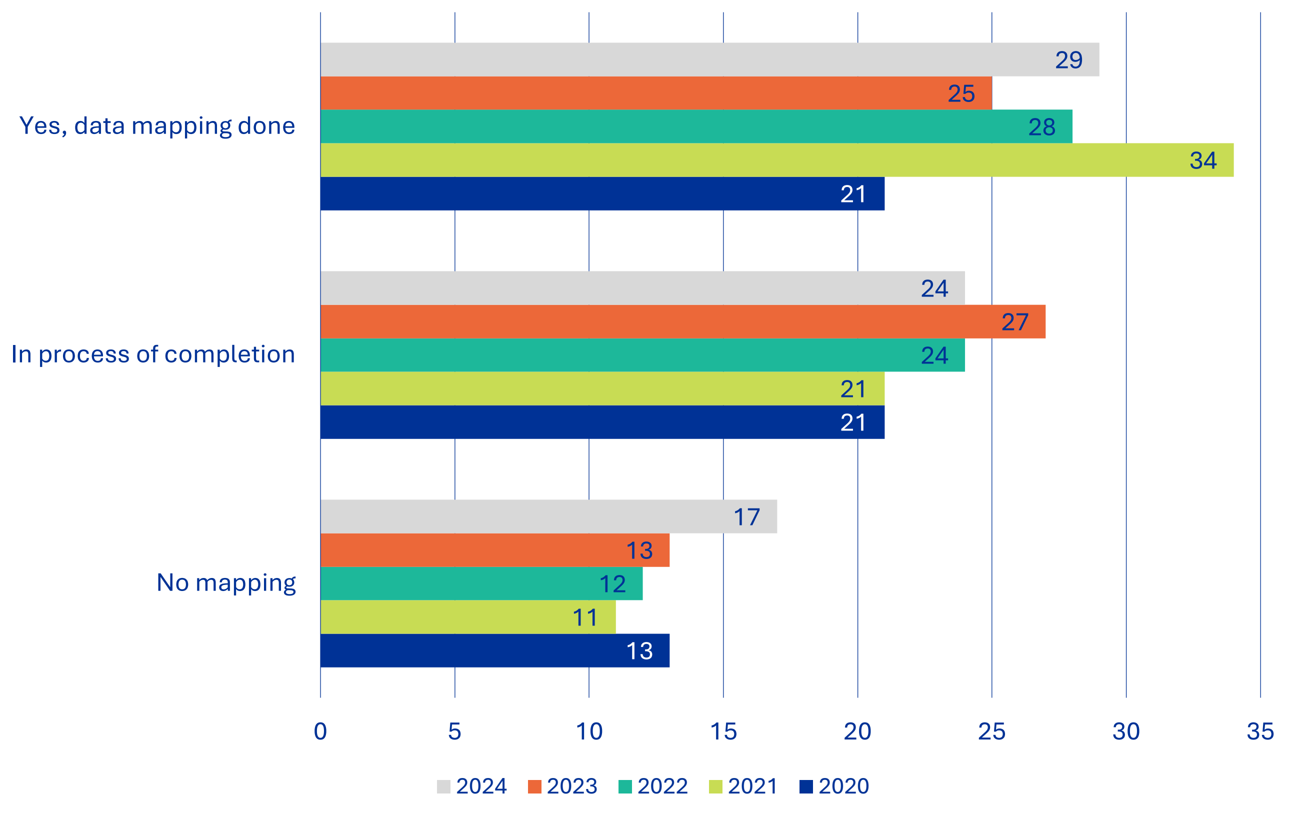
Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

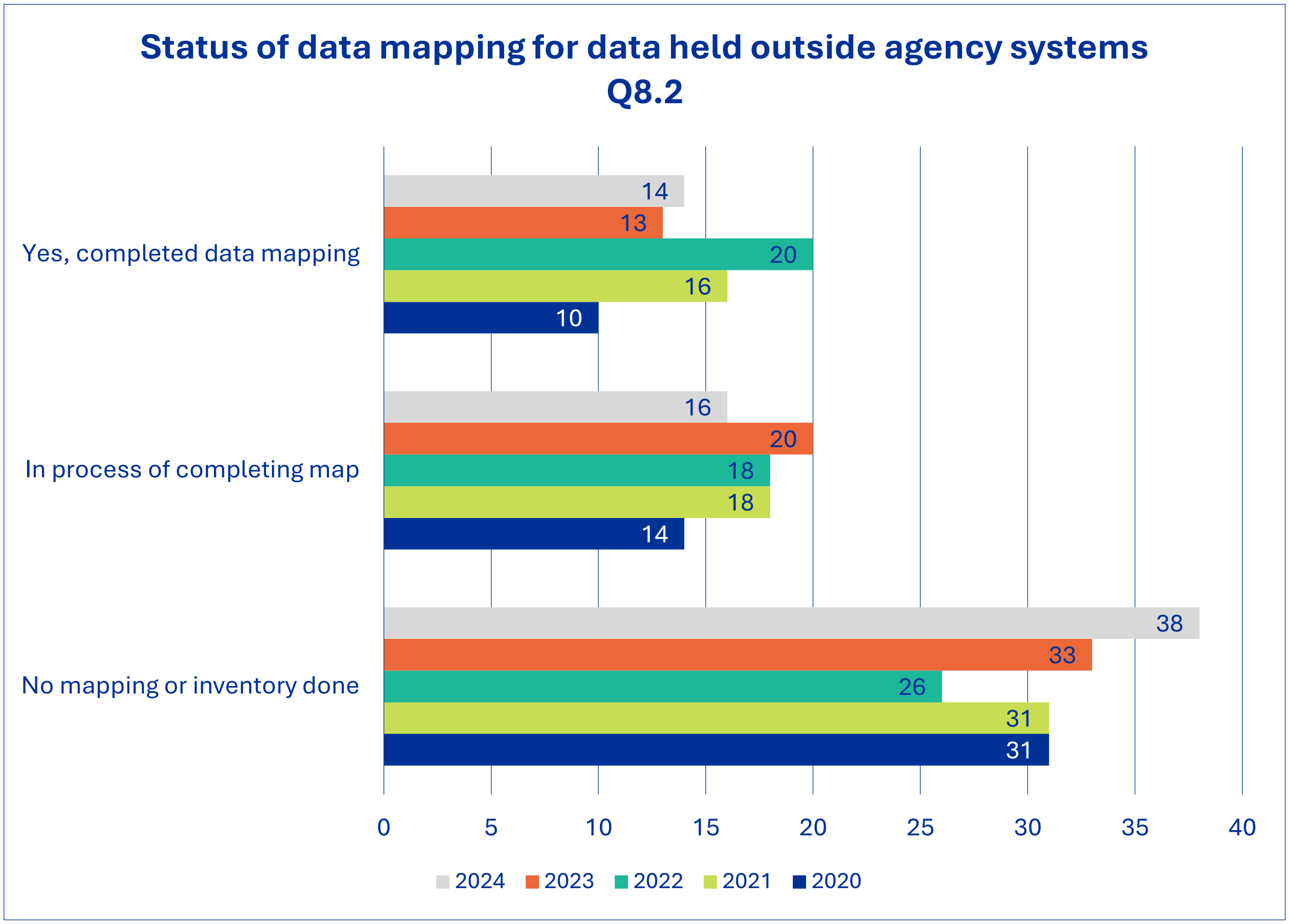
Recognizing that data inventories can be difficult to accomplish, and are often more complex than expected, the OPDP survey asked agencies about mapping data in two places – within agency systems and applications, and outside of agency systems and applications.

The chart for question 8.1 shows a year-to-year comparison of agencies that have completed a data mapping or an inventory of information *within* agency systems and applications. The 2024 data reflects completion of data mapping activities that were underway last year.

The chart for 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. Two agencies indicated "other" in their responses – one is modernizing systems and doing the mapping in that effort, and the other agency uses support organizations for the mapping of data.

Status of completed agency data mapping or inventory Q8.1



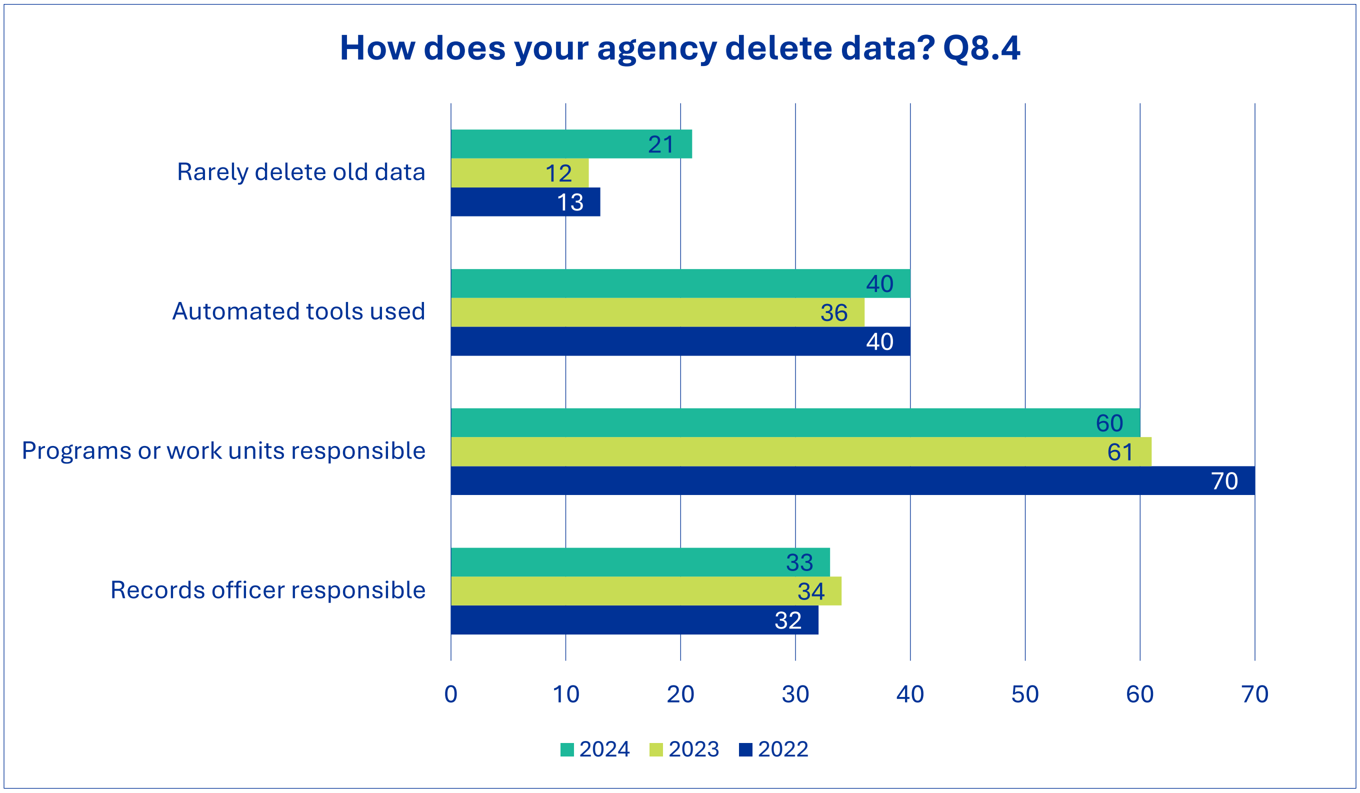


The process of data management and data inventorying offers organizations an opportunity to implement data minimization strategies and delete unneeded data. This process can also lead to cost savings and reduces risk and liability (less data means less cost to store and protect data). In asking agencies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

Most agencies have data deletion processes in place. It should be noted that agencies that rarely delete old data may be required by statute to hold old data. In 2024, across state government:

- 21 agencies rarely delete old data.
- 33 agencies have their records officer delete data.
- 40 agencies use automated tools to delete data.
- 60 agencies have individual work groups or programs responsible for deletion.

Note: agencies could choose more than one method, so totals add up to more than 70 respondents.



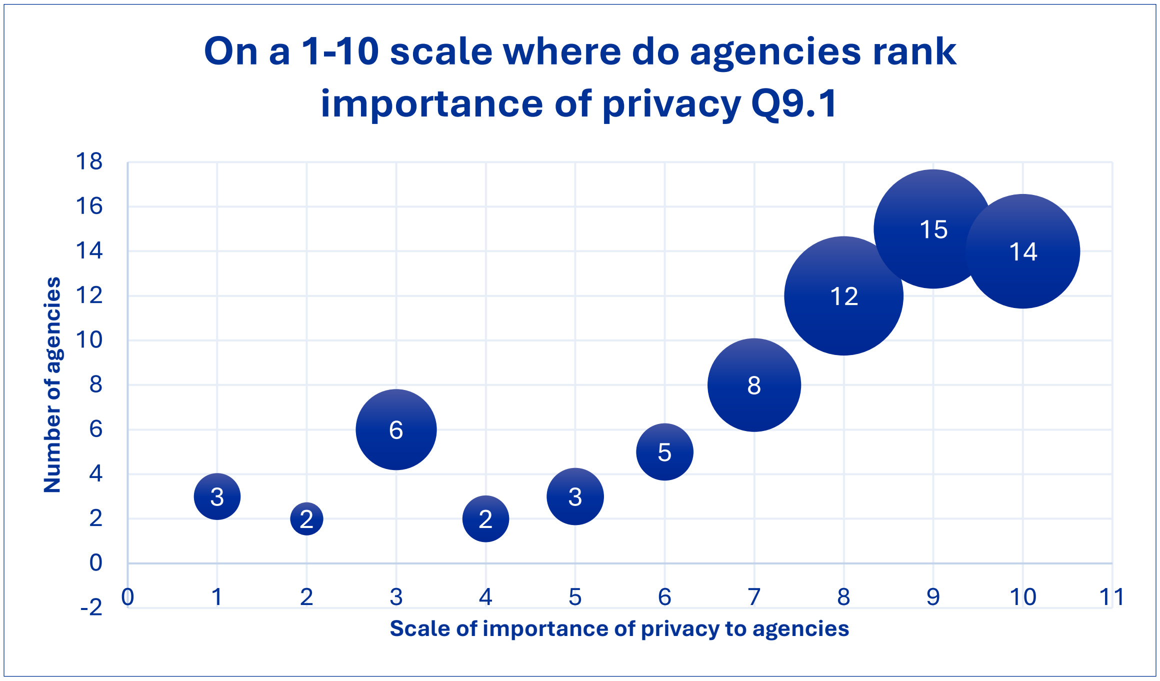
Future Planning

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 the office better meet the needs of the agencies we serve.

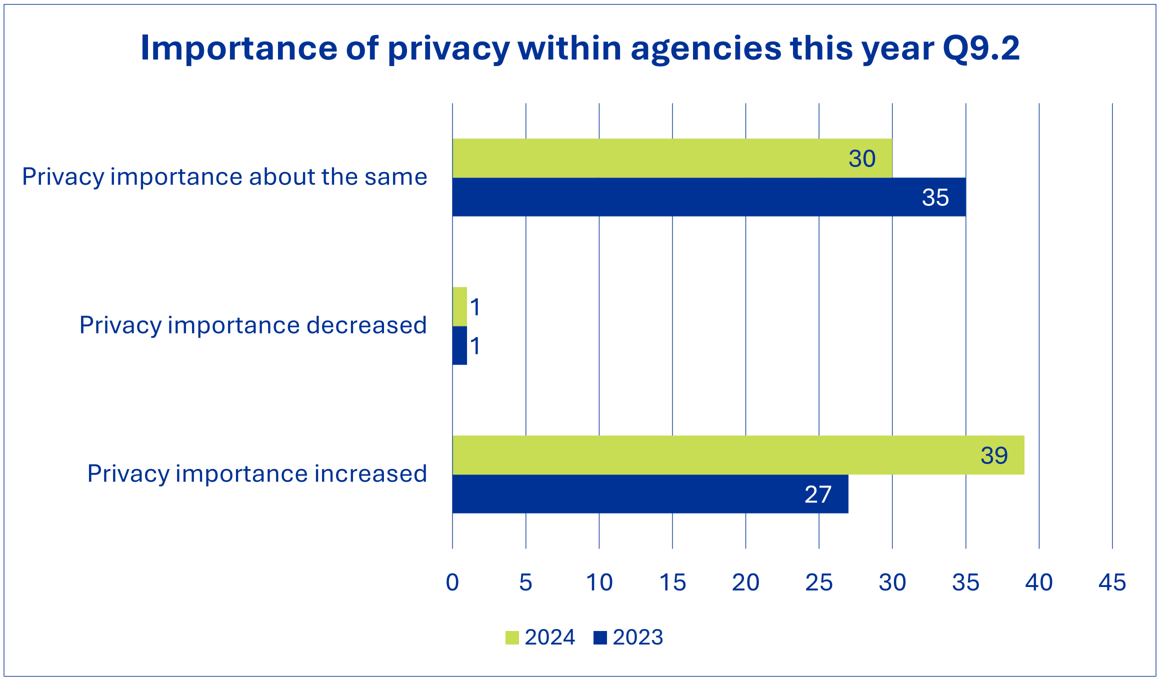
Agencies were asked about the importance of privacy to their agency, what privacy activities they already have planned over the next year, and what additional resources would be most helpful to their privacy posture.

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. Agencies have also increased participation in the OPDP webinars, trainings, and accessing other provided resources.

Agencies continue to rank the importance of privacy highly on a scale of 1-10.

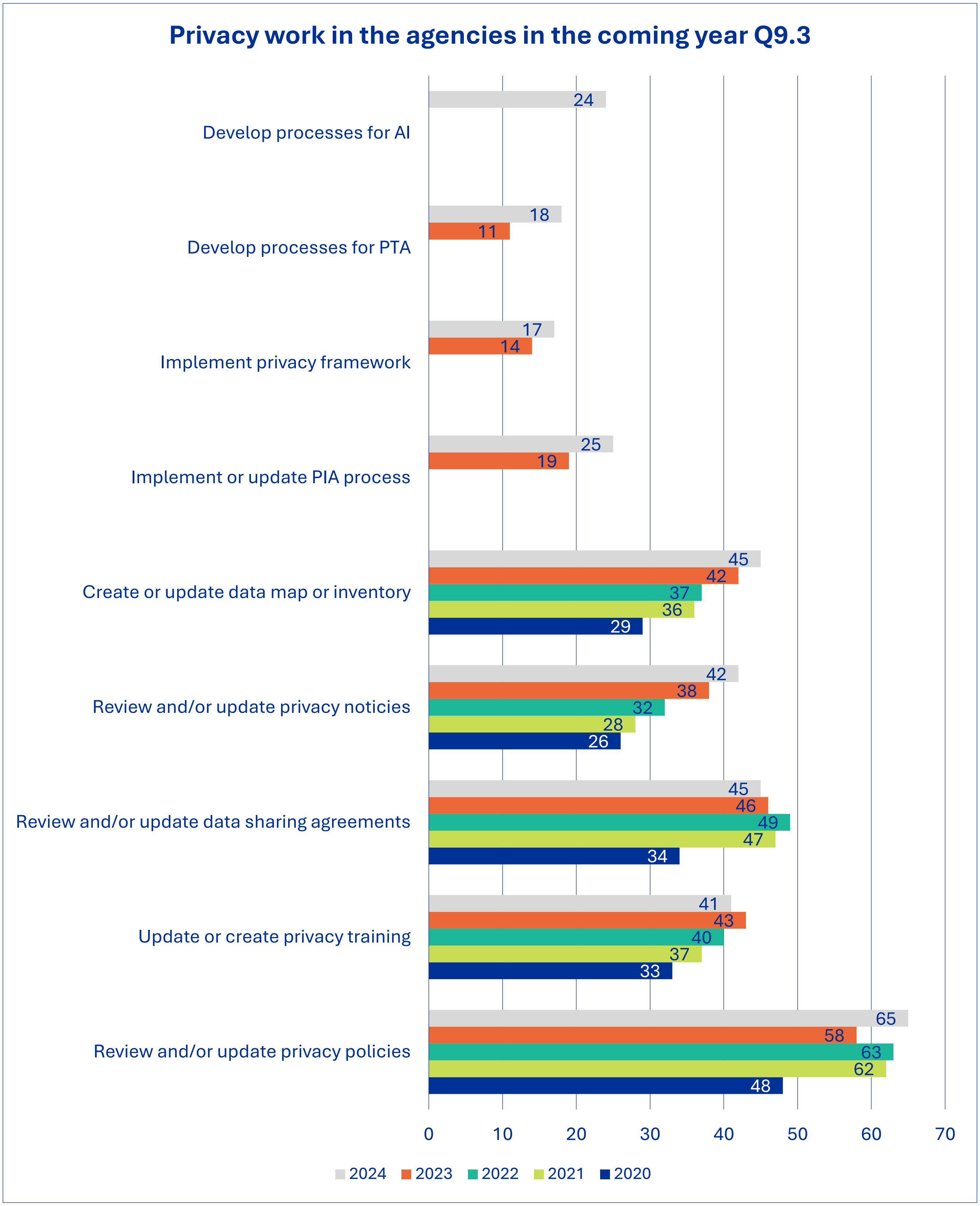


The importance of privacy is confirmed by responses of 70 agencies submitting that the importance of privacy is ongoing or has increased over the last year. Many agencies already have privacy as an ongoing important factor in their work due to long standing state or federal law.



There is an active and diverse set of work planned for 2025 as reported in the 2024 survey.

Important work around Privacy Threshold Analysis, implementing the Washington State Privacy Framework, and Privacy Impact Assessments will continue across the enterprise. One interesting new activity added this year was addressing the development of Artificial Intelligence processes and policies.



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. The four year OPDP Performance Report is also a good resource on the work of the Office of Privacy and Data Protection. It can be found here: OPDP Performance Report 2024

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.