



# 2025 State Agency Privacy Assessment

April 1, 2026

Office of Privacy and Data Protection

---

## Table of contents

Introduction .....	3
Participation and methodology .....	4
Types of personal information.....	6
Privacy roles and staffing .....	9
Agency privacy policies .....	10
Agency training.....	12
Transparency .....	14
Individual participation.....	16
Accountability.....	17
Measuring Privacy .....	20
Data sharing, third party management, and data publishing .....	22
Data inventory and data deletion .....	24
Future planning.....	27
Contact .....	29

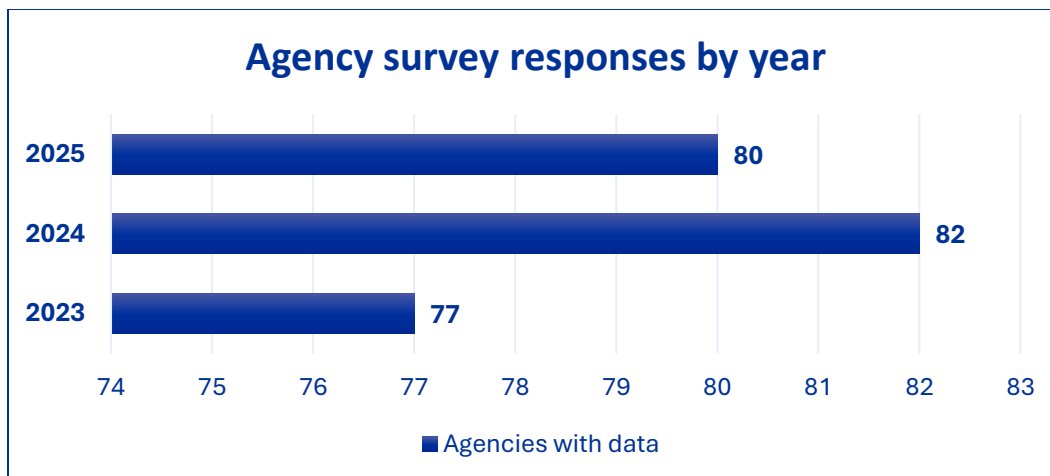
## Introduction

Under RCW 43.105.369, the State Office of Privacy and Data Protection conducts an annual review of state agency privacy practices. The required agency privacy survey helps OPDP assess privacy maturity across agencies and identify where guidance, resources, and training are most needed. The survey is intended to provide a clear understanding of current practices, not to measure compliance with specific laws or standards.

This year’s survey results show continued progress in the implementation of privacy protections, the growth of privacy awareness, and the advancement of privacy maturity across state agencies. Many practices in place in Washington have been replicated in other states based on the success at agencies in Washington.

Results from the 2025 survey show that the state continues to make progress in the implementation of privacy protections, privacy awareness, and overall privacy maturity. OPDP believes this improvement reflects greater awareness, stronger available resources, increased cross-agency collaboration, and support from both the Governor and the Legislature. Survey findings show a consistent pattern of general improvement over the past five years.

The 2025 assessment covers many of the basic components of a privacy program and aligns with the OPDP developed [Washington State Privacy Framework](#), and the [Washington State Agency Privacy Principles](#). Washington state was one of the first states in the nation to develop state specific privacy principles, 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.



The chart above shows 3 years of agency participation in the survey. Agency participation in the 2025 assessment was similar to 2024, with 80 state agencies responding this year, compared with 82 in 2024 and 77 in 2023. Of the agencies that responded in 2025, 67 reported holding personal

data and 13 reported that they do not. The analysis in this report is based on the 67 agencies that hold personal data.

The legislative branch did not submit survey responses in 2025. In prior years, legislative branch agencies accounted for nearly a dozen responses. At the same time, small agency participation increased, due in part to a new OPDP staff position focused on small agency privacy. Year-to-year variation is also affected by some small agencies submitting combined responses with larger support agencies.

Despite these shifts in participation, the data continues to provide a strong view of 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. This evolution is most evident as Artificial Intelligence use expands.

## Participation and methodology

The State Chief Information Officer sent the annual assessment to agencies as part of the [2025 annual technology certification](#) process. Each year agency partners are required to provide information to track compliance with statewide technology policies.

Sending the privacy assessment survey with the annual certification process helps with consistency for WaTech and state agencies in the collection of responses.

Personal information – 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 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

The assessment provides useful information about agency privacy practices, but it is limited to what can be measured in a survey. For example, it can show whether an agency has formal policies and staff training, but it does not judge how strong those policies are or how well the training works.

The data in this report is used to give an annual statewide view of privacy practices across governments, not to evaluate individual agencies.

In 2025, 41 agencies reported that privacy had become more important, the same number as in 2024. Survey results show that privacy has remained a high priority across state government since 2021, when 86 percent of agencies reported that strong privacy practices were important.

Very few agencies have reported that privacy became less important. In 2022 and 2024, only one agency reported a decline in the importance of privacy. In 2023 and 2025, no agencies reported that privacy had become less important.

OPDP believes this continued emphasis reflects growing awareness of privacy issues, state action on new privacy laws, media attention to privacy protections in the private sector, and ongoing discussion about artificial intelligence.

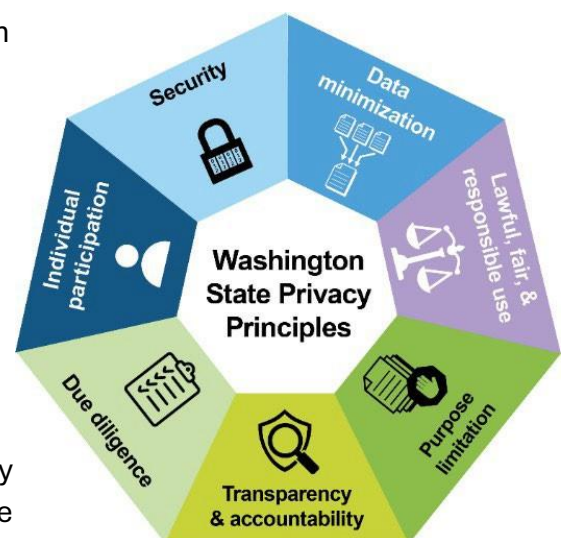
A note about the charts in this report. The numbers indicate the number of agencies that responded and held personal data: 67 of 80 in 2025. The charts are labeled with the question number on the survey in order to cross reference the data more quickly.

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 as the use and implementation of Artificial Intelligence technology continues.

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



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.

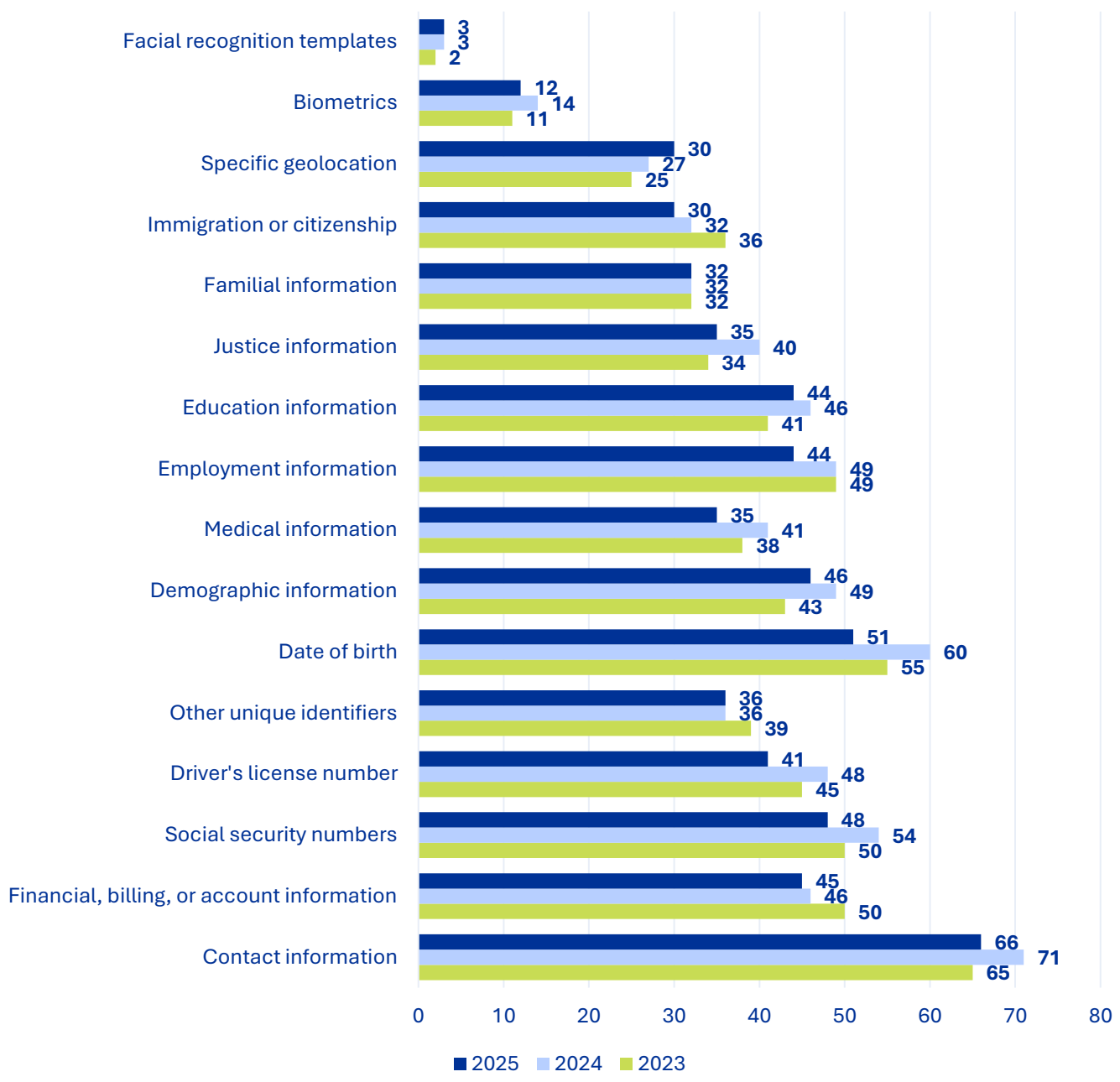
In 2025, OPDP continued to produce [resources](#) for state, local and Tribal governments. These resources include the new [Washington Privacy Framework: Building a Foundation for Your Privacy Program](#) course that provides the essential structure and concepts needed to build an effective privacy program. OPDP also led the discussion on Artificial Intelligence (AI) technology and privacy with eight presentations, and involvement in the state’s [AI Taskforce](#). The year culminated in an outside [Joint Legislative Audit and Review Committee \(JLARC\) report](#) that looked at the work and success of OPDP. JLARC found “The Office of Privacy and Data Protection (OPDP) meets statutory responsibilities and receives high user satisfaction.” And “82% of state agency staff who use OPDP resources said it met all or most of their needs”.

## 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. There were no large shifts in the responses regarding the kinds or types of data maintained by state agencies.

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.

### Types of data held by agencies Q1.1



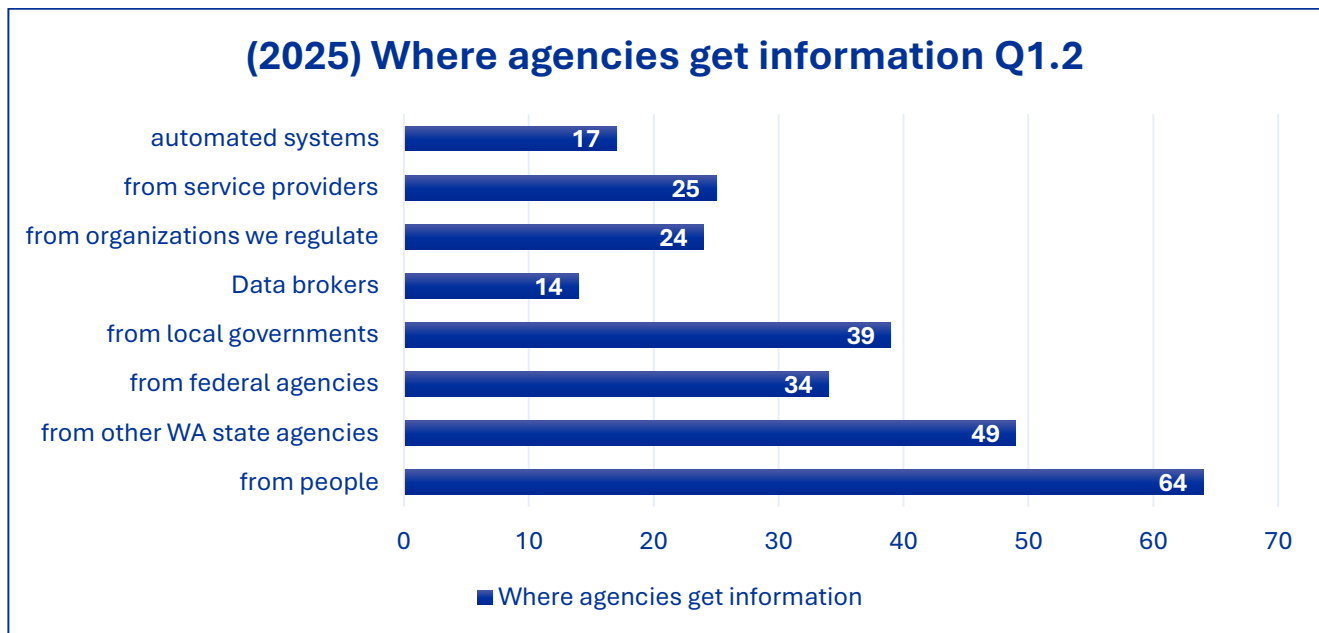
The type of information agencies maintain is important as a determination for the type of privacy controls needed to minimize risk and appropriately protect the information. It is important to note that the context of the data held is also important in how it is protected by an agency.

The types of information that agencies maintain varies widely. In 2025, contact information is again the most common type of information held by agencies (66 agencies).

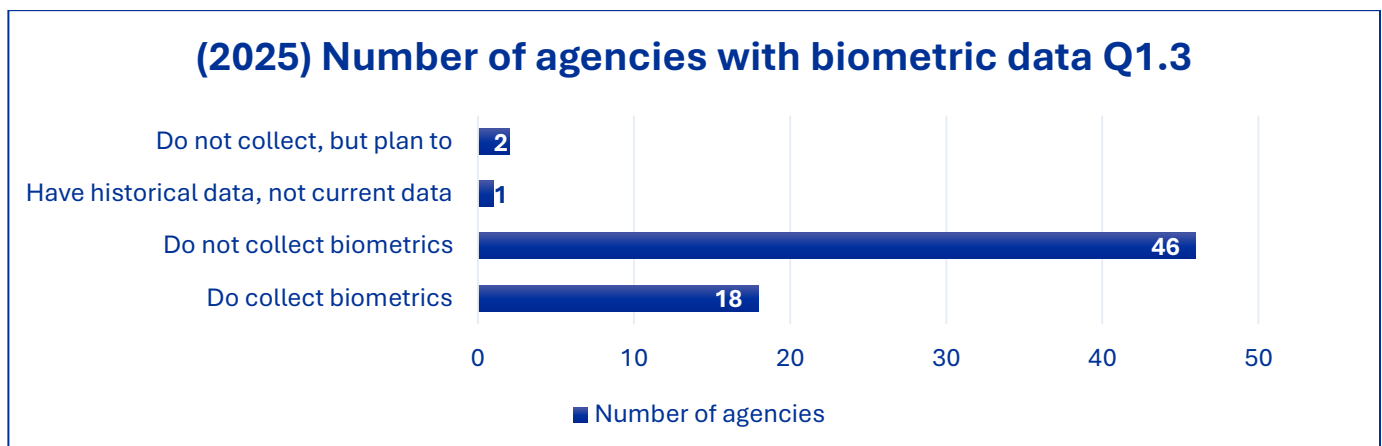
The survey only represents the most common types of data collected across state agencies. Individual agencies may collect information required by law, or for implementation of their mission.

For example, some individual agencies reported collecting data in these categories: incarceration status, date of death, number of children, banking information, training or certifications held, active investigation information, student IDs, last four of social security numbers and contractor background checks.

The next question in the survey asked where agencies get the data they hold. Sixty-four agencies reported they get the data from people (to provide services, or as required by law.) Only 17 agencies reported they receive data from automated systems, and 49 agencies get their data from other Washington state government agencies. All agencies are required to have data sharing agreements in place for these types of exchanges.



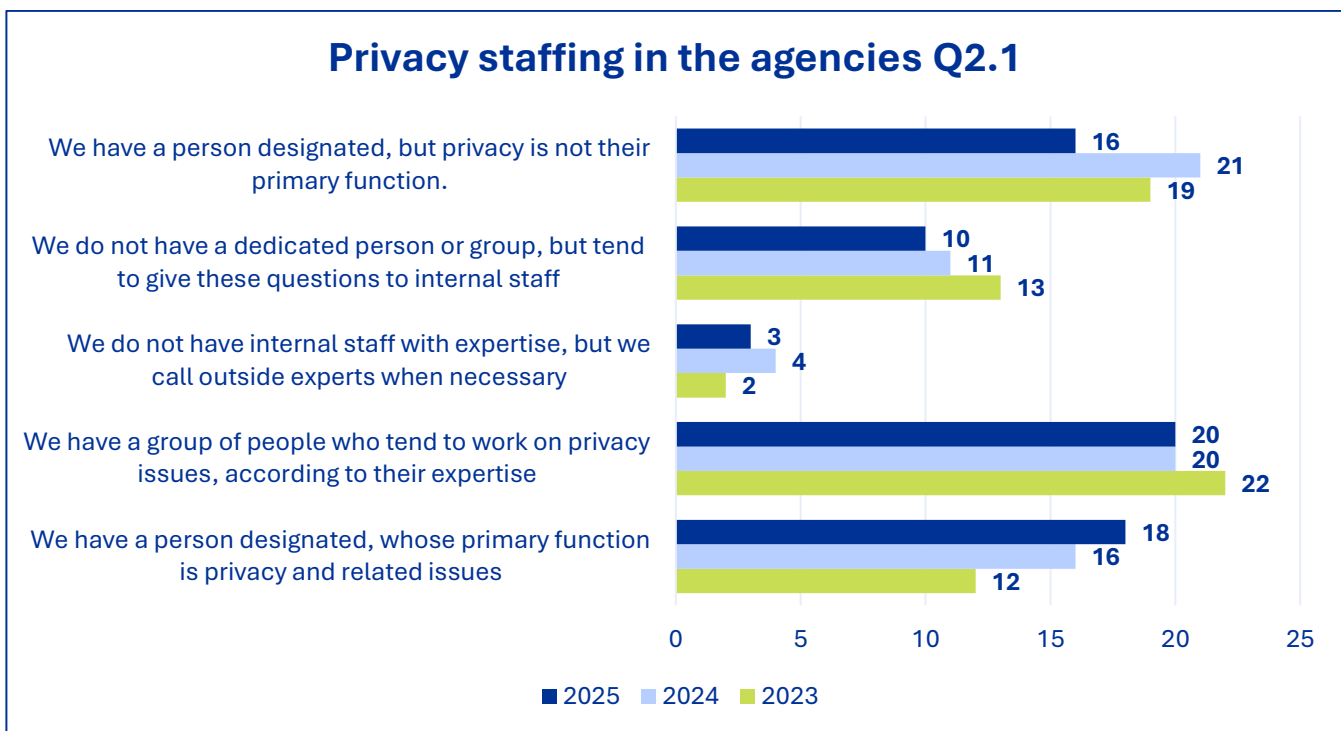
There continues to be an interest in the policies around biometric data. In 2025, 46 agencies reported they do not collect any biometrics. Eighteen agencies reported they do collect biometric data, and two agencies are currently in the process of developing standards or policies for collecting biometric 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 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 2025, 34 of 67 agencies said they had a specific person assigned to handle privacy policy issues, either as a primary or secondary responsibility. That compares with 37 of 72 agencies in 2024 and 31 of 68 agencies in 2023.



The low number of agencies reporting that no one is assigned to privacy policy is a positive sign for the state. OPDP believes this reflects stronger awareness of privacy issues, adoption of the enterprise privacy and AI policies, and broader access to privacy training and resources.

Even when an agency does not have a designated privacy lead, privacy responsibilities are often shared among staff such as information security staff, information governance staff, risk managers, and records officers. OPDP supports all of these roles 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. Privacy practices are a journey of constant improvement, and consistent staffing helps this path towards more maturity.

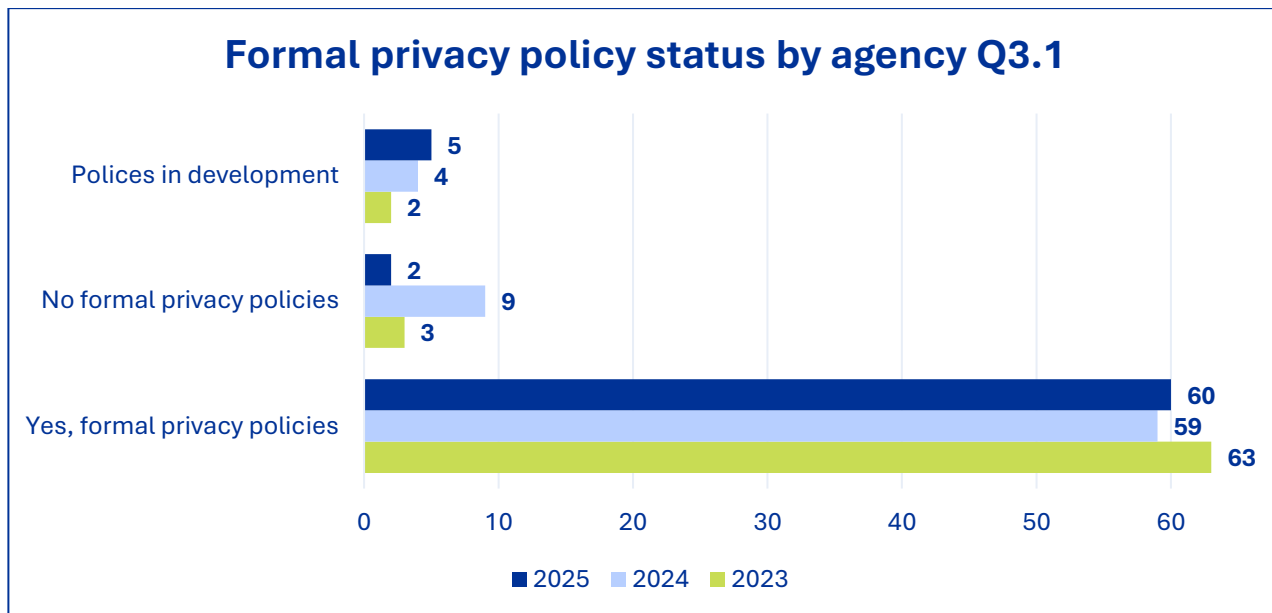
OPDP has developed and implemented training for the enterprise that can be utilized by personnel in any discipline. This enhances privacy protections at any step on the path towards maturity. Dedicated staffing within agencies allows the OPDP to better target assistance for customer agencies with privacy 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 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, 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 for three years in a row.

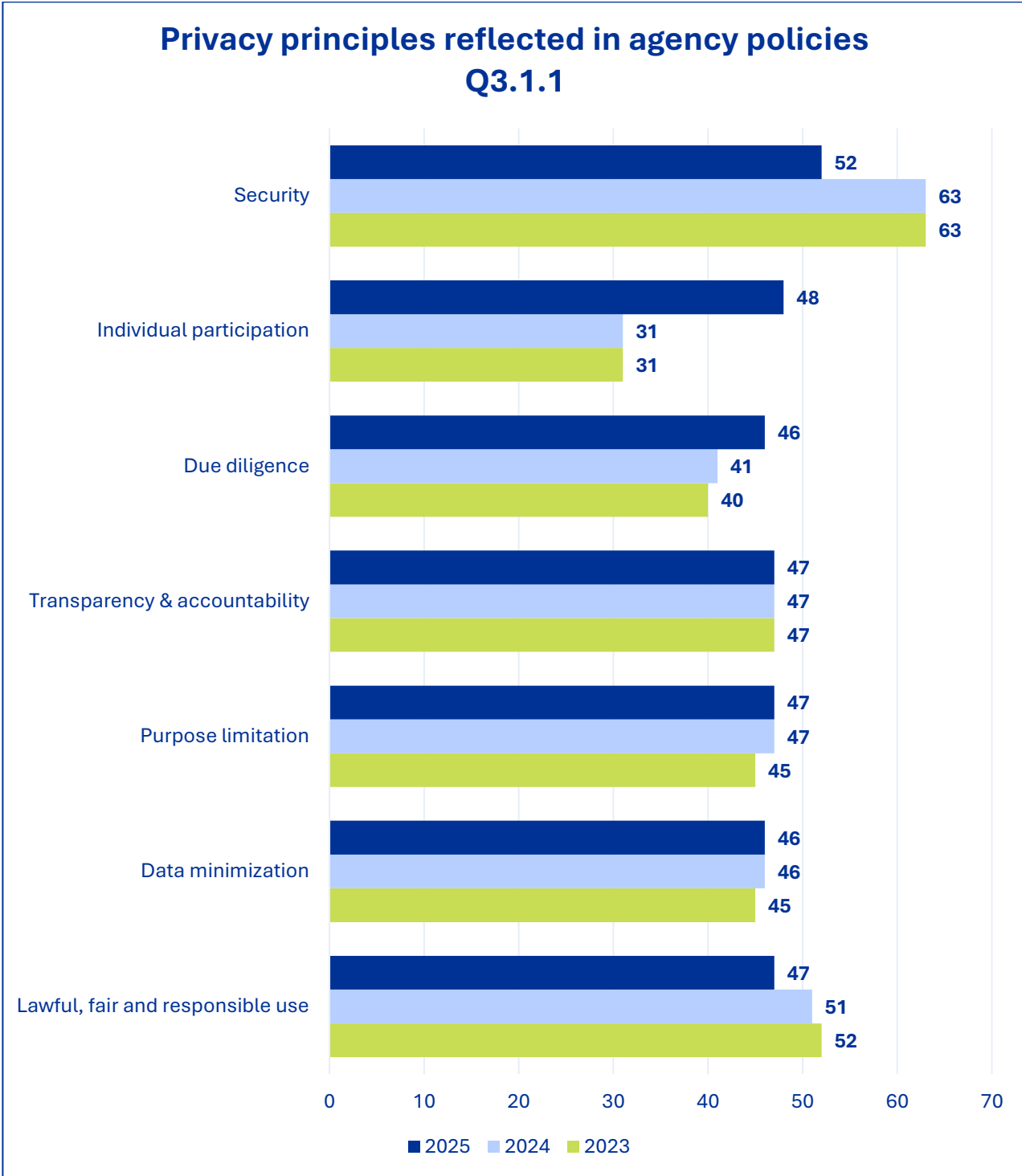
## Agency privacy policies

State agencies that maintain personal data are implementing the Washington State Privacy Principles and the Washington State Privacy Framework for agency data protection.

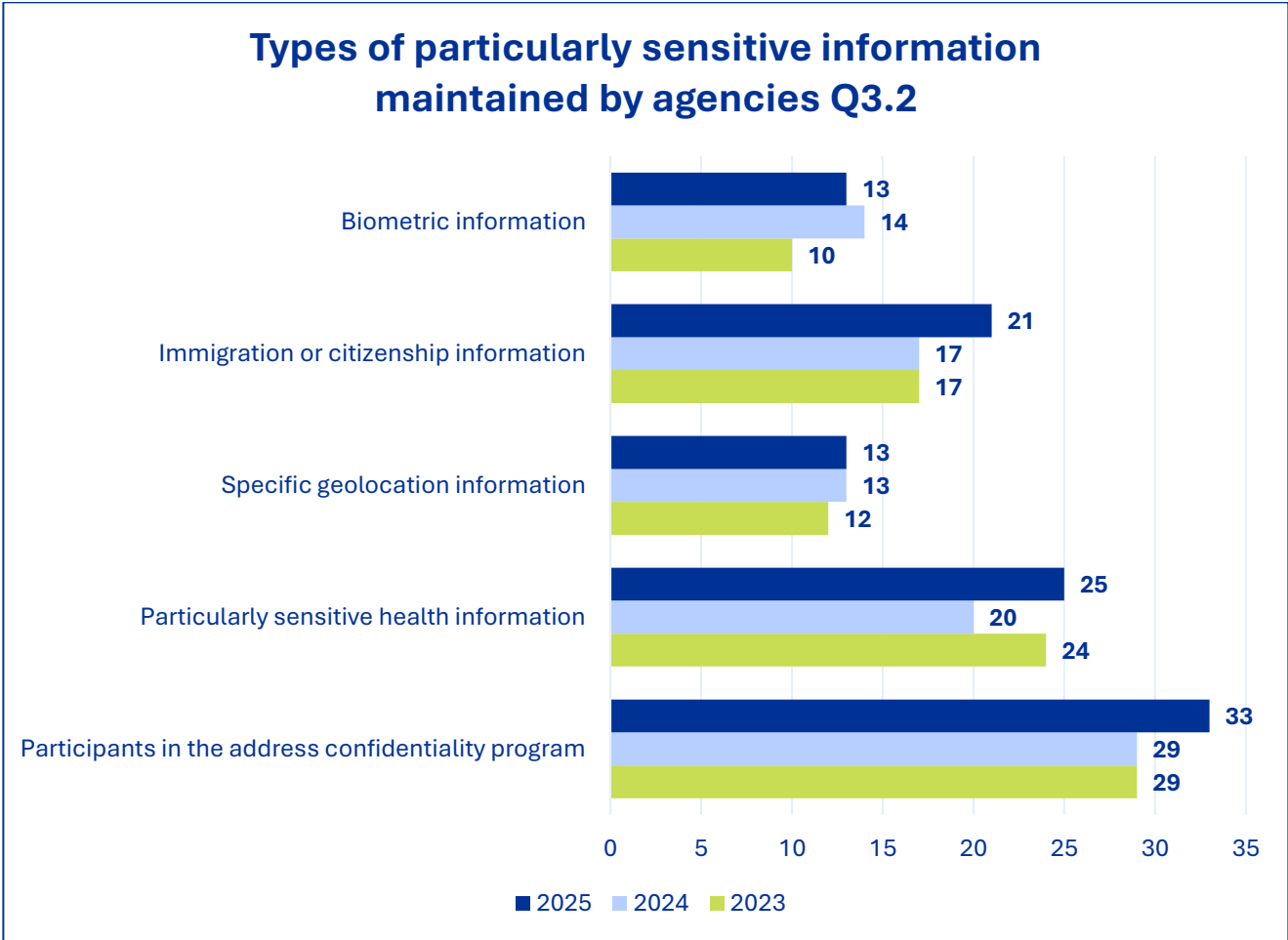
Internal agency privacy policies apply to how information is collected, used and shared. Policies demonstrate that an agency understands the protections that apply to its information and has implemented appropriate standards. Policies are also one way to document the agency’s commitment to how it will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



There are two factors driving adoption and implementation of formal privacy policies: 1) The newly adopted enterprise privacy and data policy and 2) the greater awareness and importance of privacy. Both factors have resulted in more policy development across state government. Support from legislative and executive branch leadership has also been crucial.



The state privacy principles guide specific privacy policies within state agencies. The above chart shows, year over year comparisons are consistent across the privacy principles reflected in agency policy. The “Security” privacy principle is the one principle reflected in the most agency policies or standards.



The survey drilled into the exact kinds of data that is protected by policy. The specific kinds of data protected by policies, procedures or standards 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.

### 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.

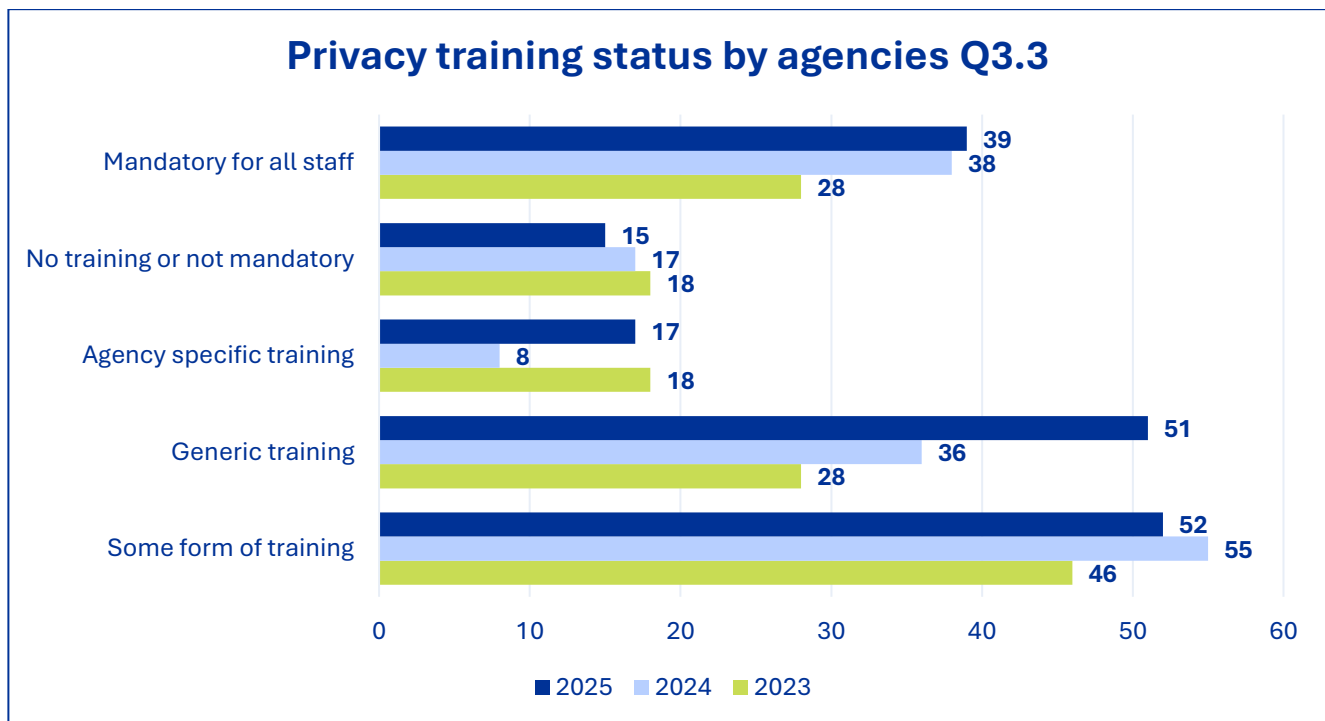
The OPDP developed statewide training to help agencies build awareness of the importance of privacy. This Privacy Basics training for state employees is available to all state agencies through the enterprise learning center or via the [OPDP website](#). The training is also being piloted to local governments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

In addition to web-based training, the 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 2025 responses indicate a majority of agencies offer some form of training. This is consistent with past year’s 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 52 agencies that offer training, 51 agencies reported generic privacy training, and 17 reported agency specific training. More agencies require privacy training now than in the past. More agencies are also making privacy training mandatory for employees.

Last year, OPDP identified training as an area to watch as its state-developed privacy training was adopted across the enterprise. That growth occurred in 2025, with more employees receiving

training as agencies used OPDP’s materials. OPDP made development of a statewide privacy training program a priority based on findings from earlier surveys.

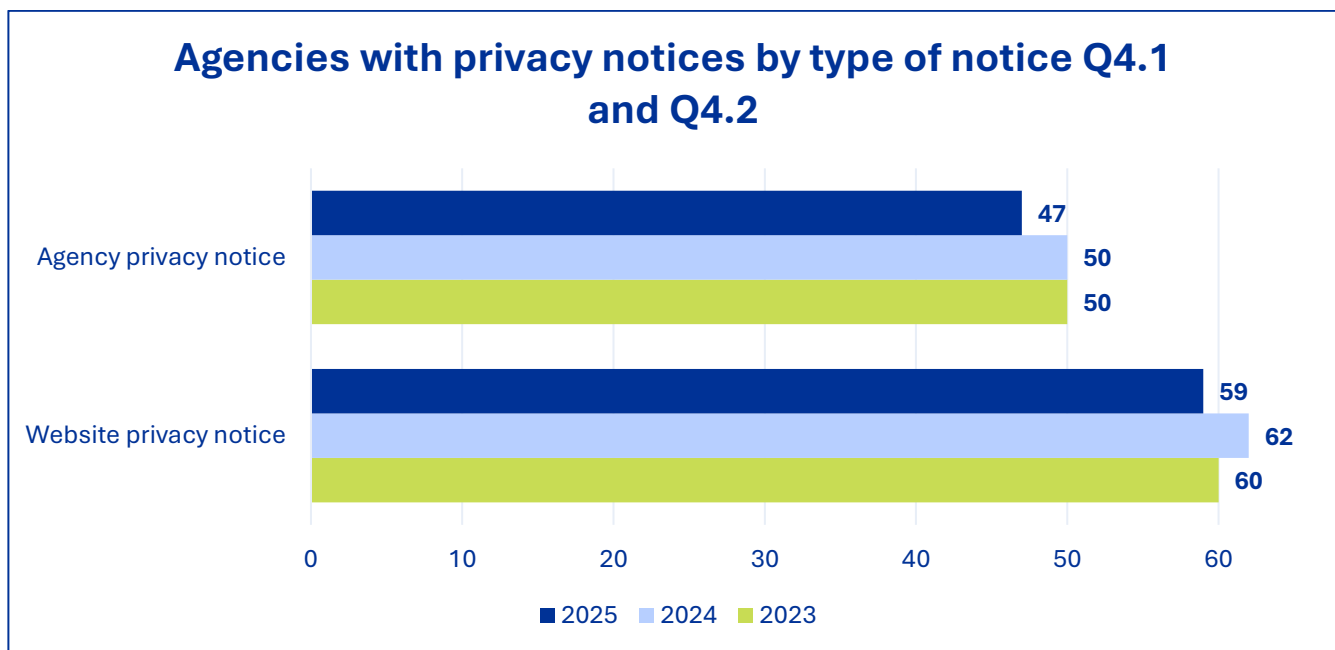
More information about use of OPDP training is available in the [OPDP Performance Report 2024](#). OPDP also continues to develop and update training through webinars and web-based modules.

## 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 focus on 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 2025, 59 agencies indicated they had a website privacy policy.

Depending on context, 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.

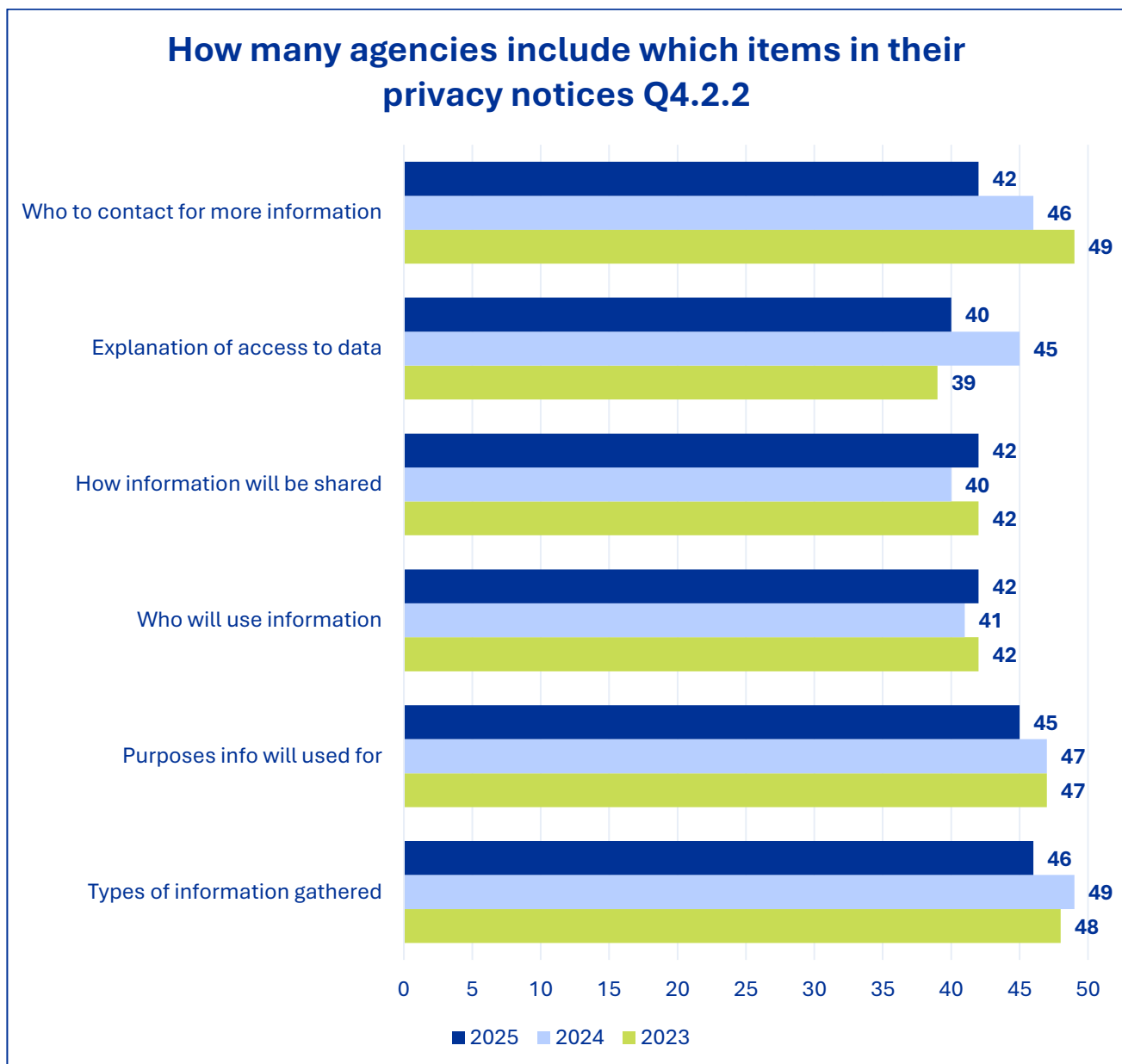


More than half of the agencies with personal information – 47 agencies – indicated they have this type of comprehensive privacy notice. Most agencies post it on their website, while some also mail the notice or provide it in-person.

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.

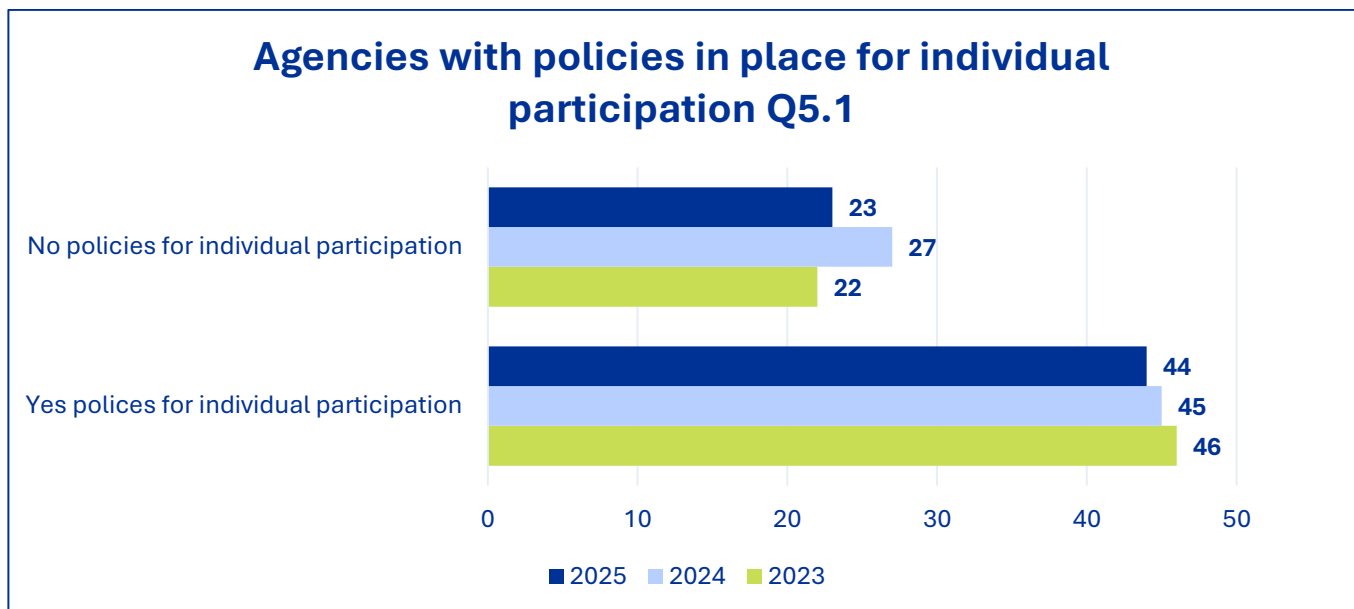


## Individual participation

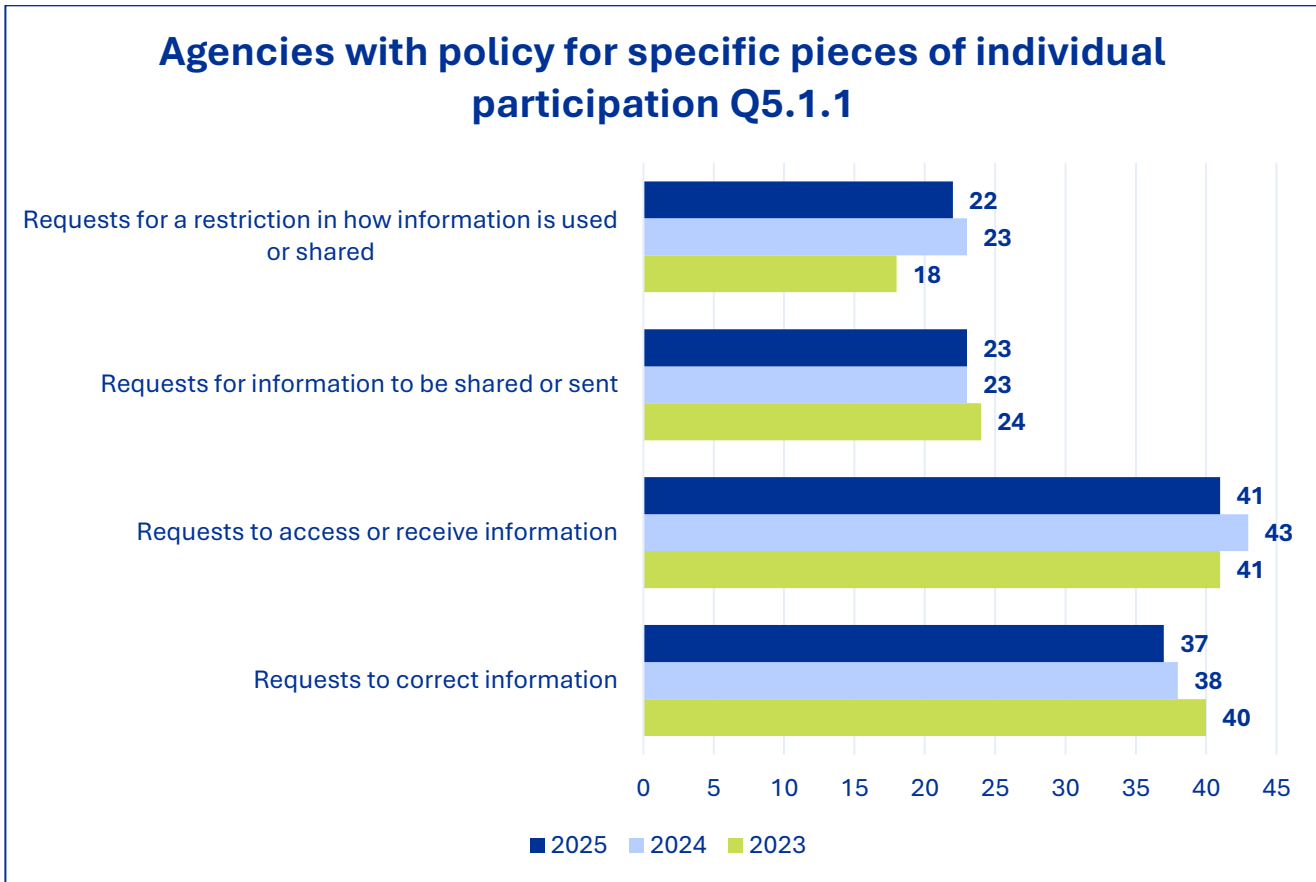
The Individual Participation principle – people should have control of their information whenever possible – can be implemented by having processes for requests:

- To access or receive information.
- To correct information.
- For information to be shared or sent to another person.
- For a restriction on 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.



The next question in the survey asked agencies that had individual participation policies what those policies addressed. The chart for question 5.1.1 shows that most agencies had a process for people to correct inaccurate information. The most common policy in place is a process for people to access or receive information, which synchronizes with 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.

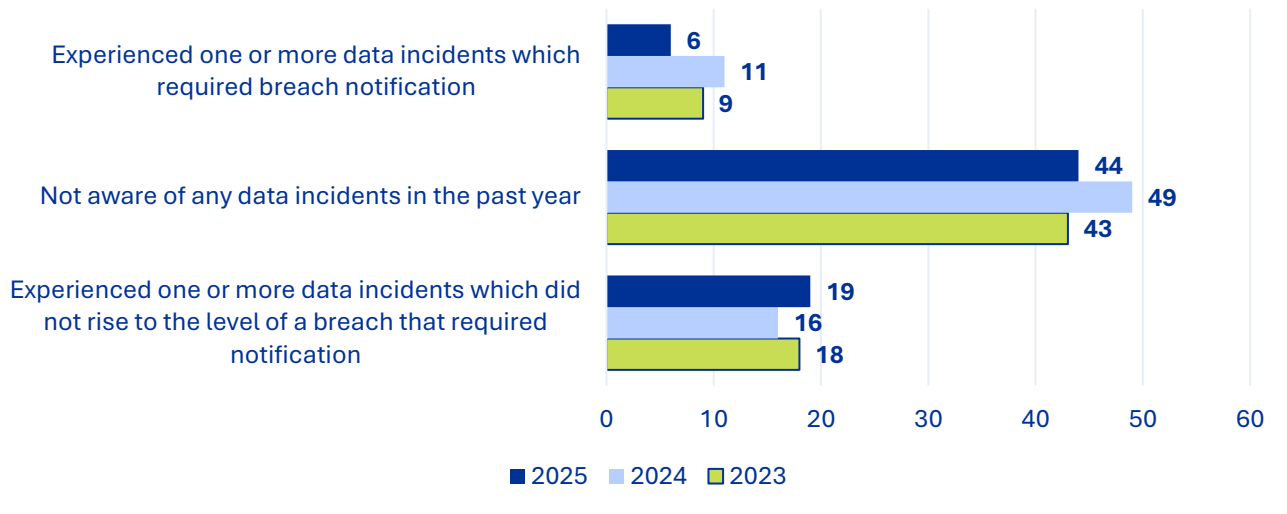
Agencies were asked about privacy incidents or breaches that occurred in the last year.

- 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.

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. This paradox is kept in mind when interpreting and designing metrics directed at achieving policy outcomes.

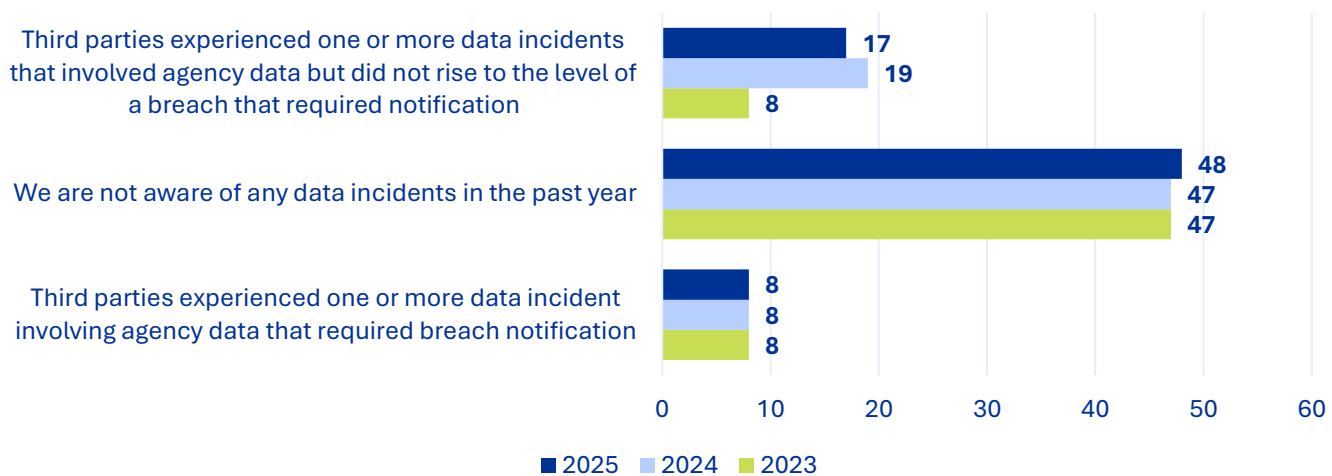
### Agency experience with data incident notification Q6.1



The OPDP has expanded assistance to agencies through a [Data Breach Assessment Form](#) to determine if an incident has occurred and next steps.

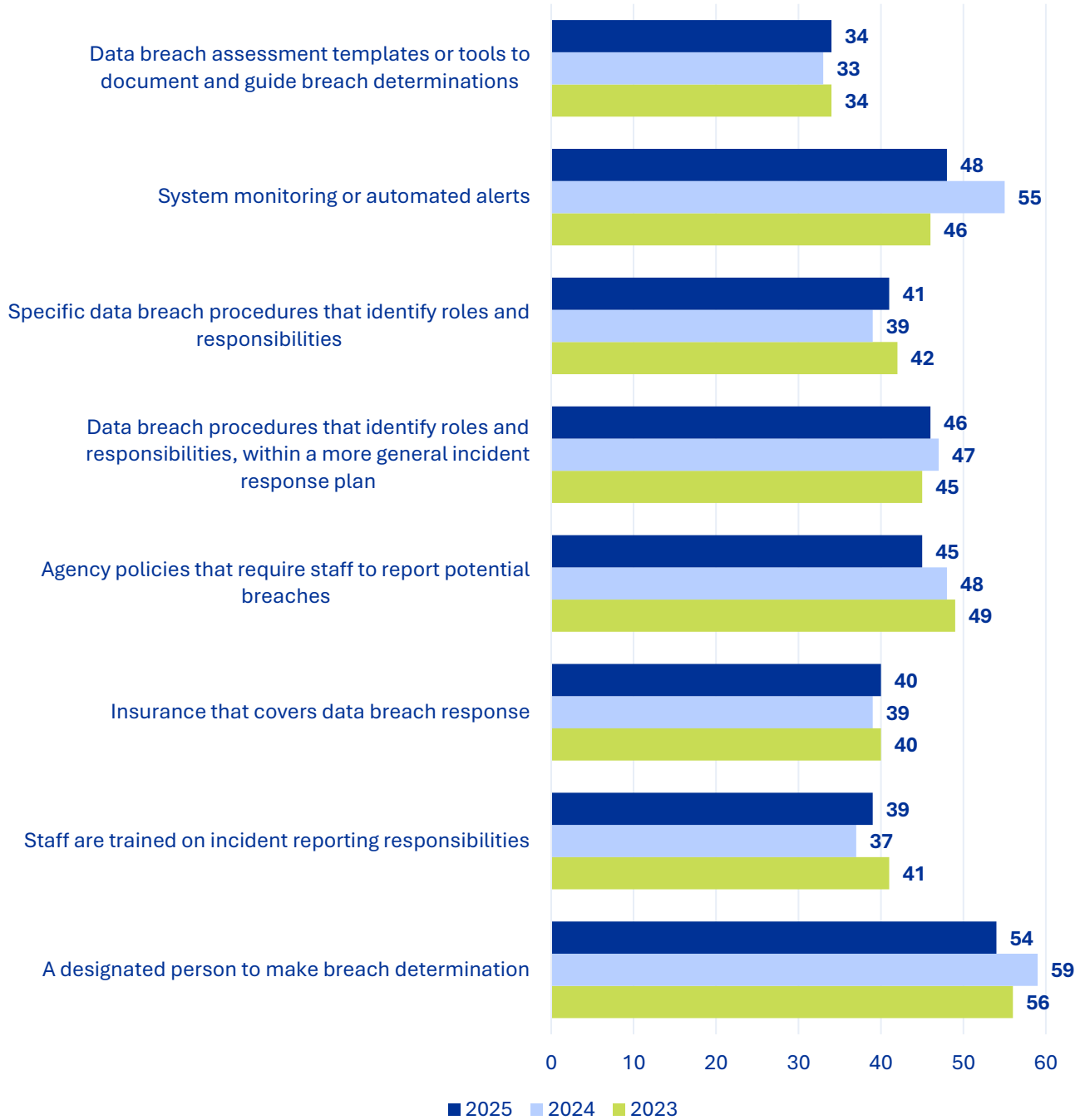
The OPDP asked agencies about incidents experienced by third parties they share information with. Third parties, such as service delivery providers, technology vendors, and researchers, have significant access to personal information. Just as agencies must appropriately protect the information they maintain,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

### Third party incidents and notification Q6.2

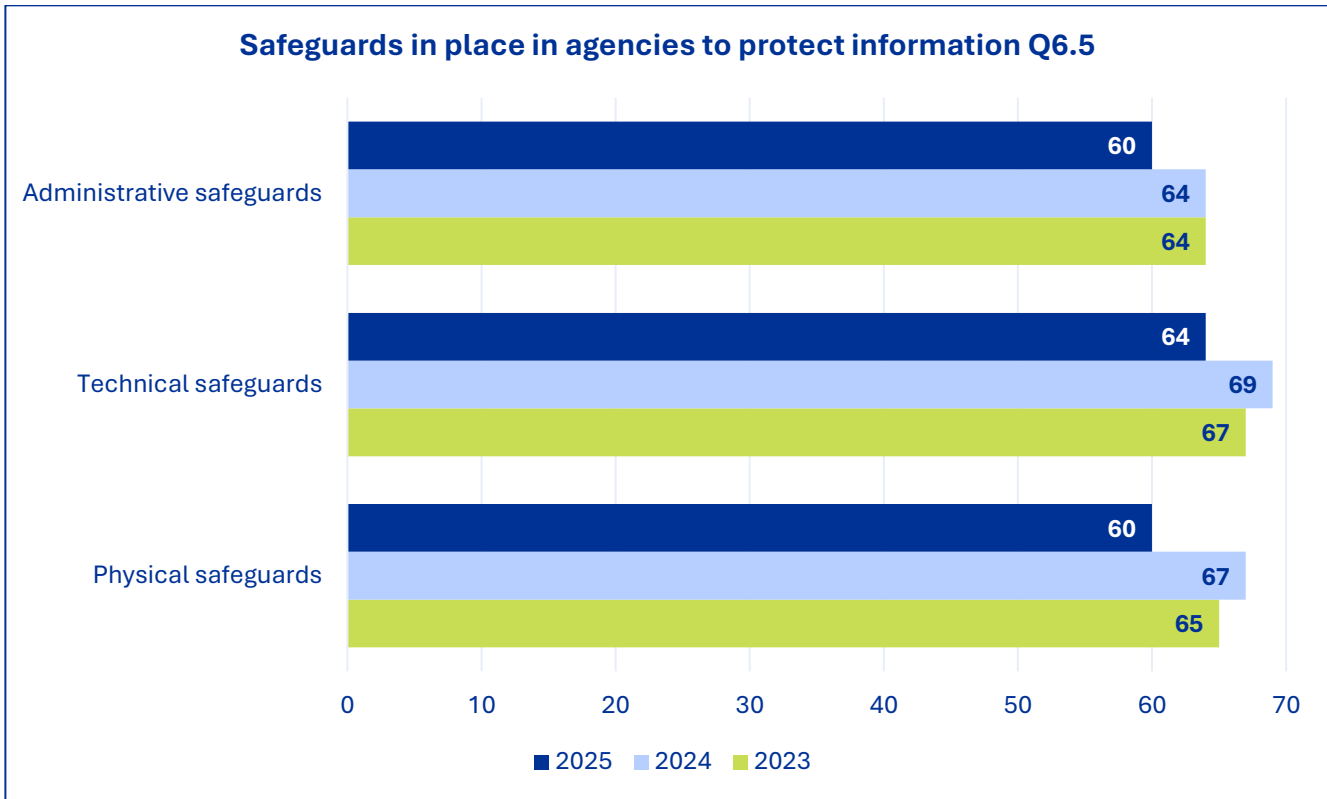


The OPDP asked agencies what steps they have taken to ensure incidents are discovered. Fifty-four agencies have designated at least one person to make breach determinations. About half of those agencies have also implemented assessment tools or templates to address possible breaches. Overall agencies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

**Agency controls for data breaches Q6.3**

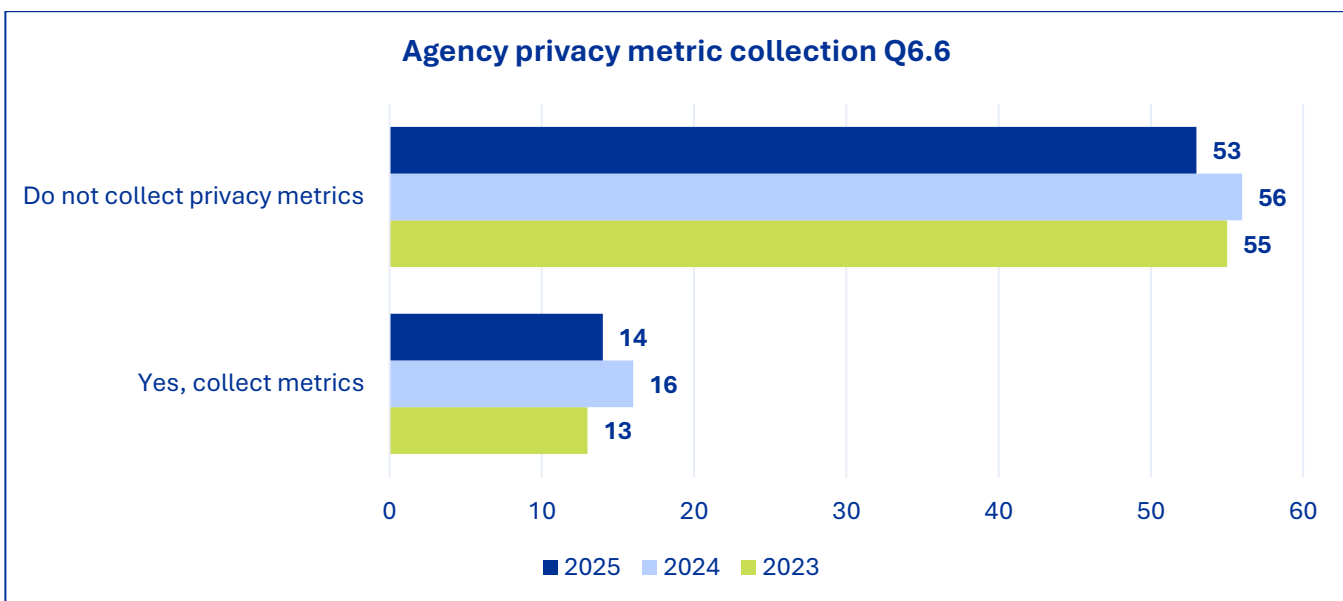


Focusing on specific kinds of controls for data protection the general assessment is positive across the state enterprise. Agencies continue to place and maintain administrative, technical, or physical safeguards for protecting data.



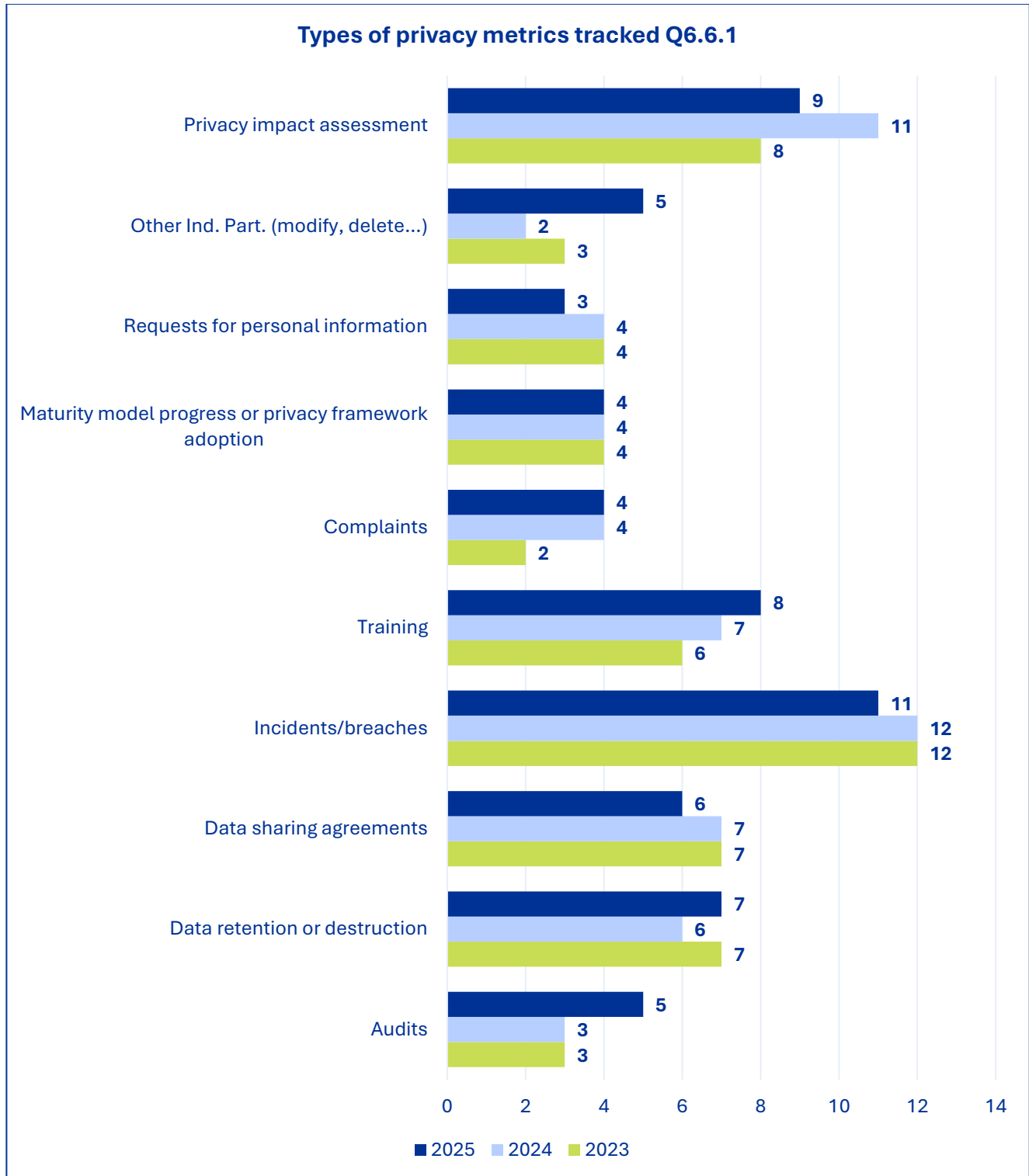
## Measuring Privacy

In 2022 questions were added to the survey about measuring data privacy. An ongoing endeavor of the OPDP is exploring the best way to measure the maturity of privacy programs beyond this annual survey. To support this effort, the OPDP offered a [webinar on privacy metrics](#), and is monitoring 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.

Agencies that do collect metrics were asked about those metrics as seen in the chart below.

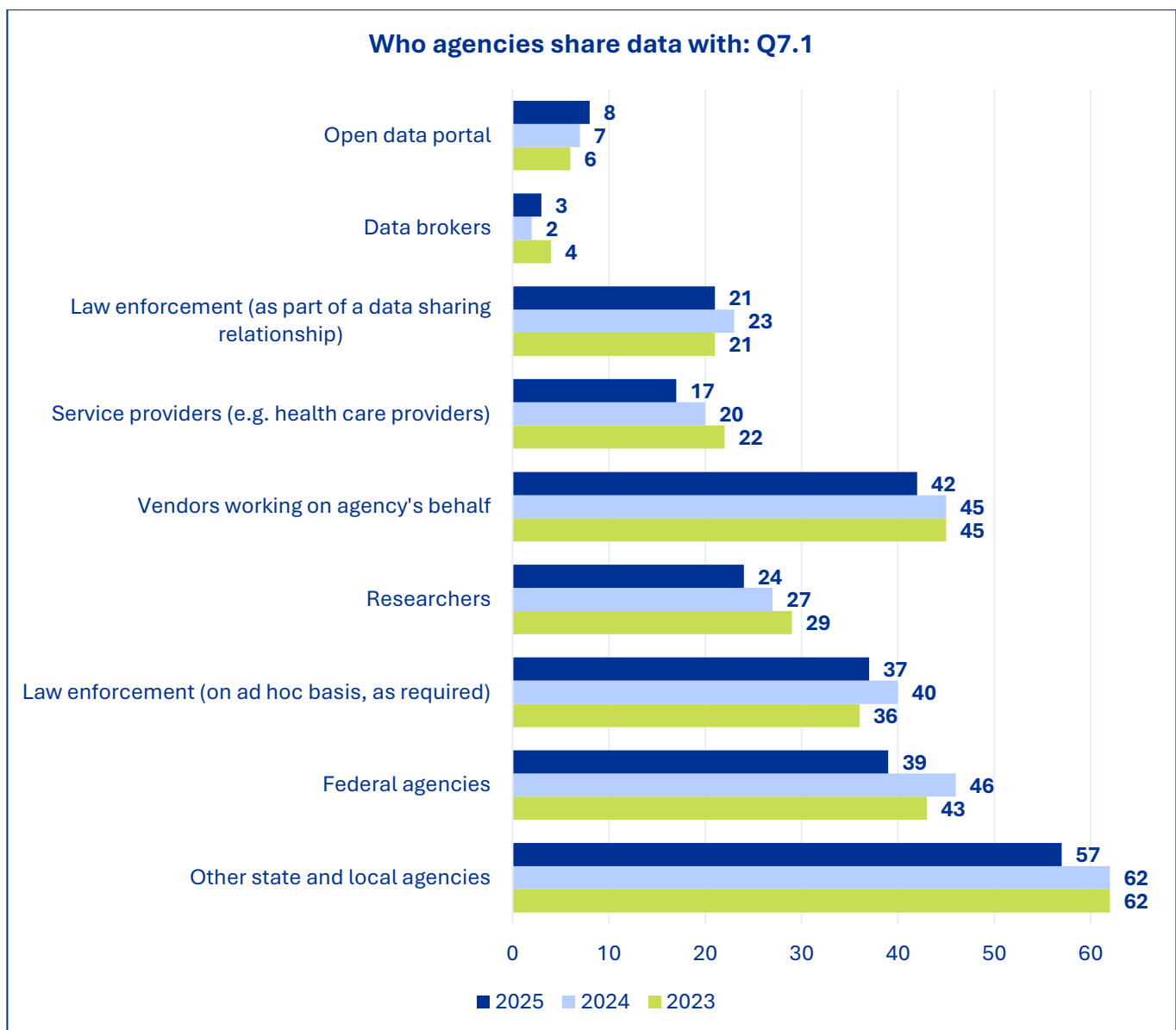


## Data sharing, third party management, and data publishing

Agencies continue to 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 while implementing their public focused missions.

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.

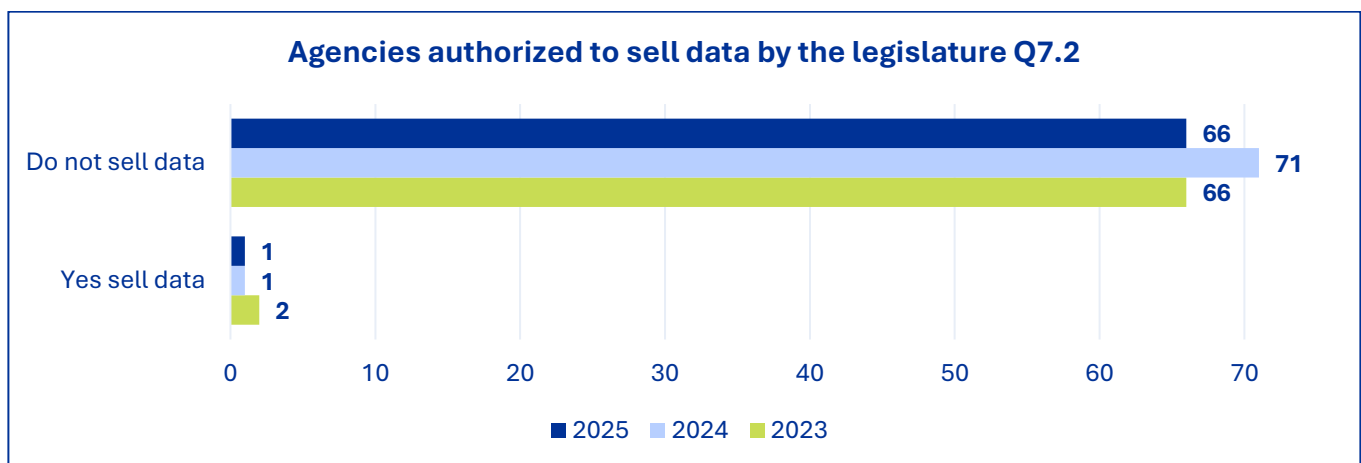
A new category of data sharing was added to the survey in 2023 after discussions with agencies. The “open data portal” was added because six agencies reported sharing with an open data portal to provide better public access to data. That number is up to eight this year.



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.



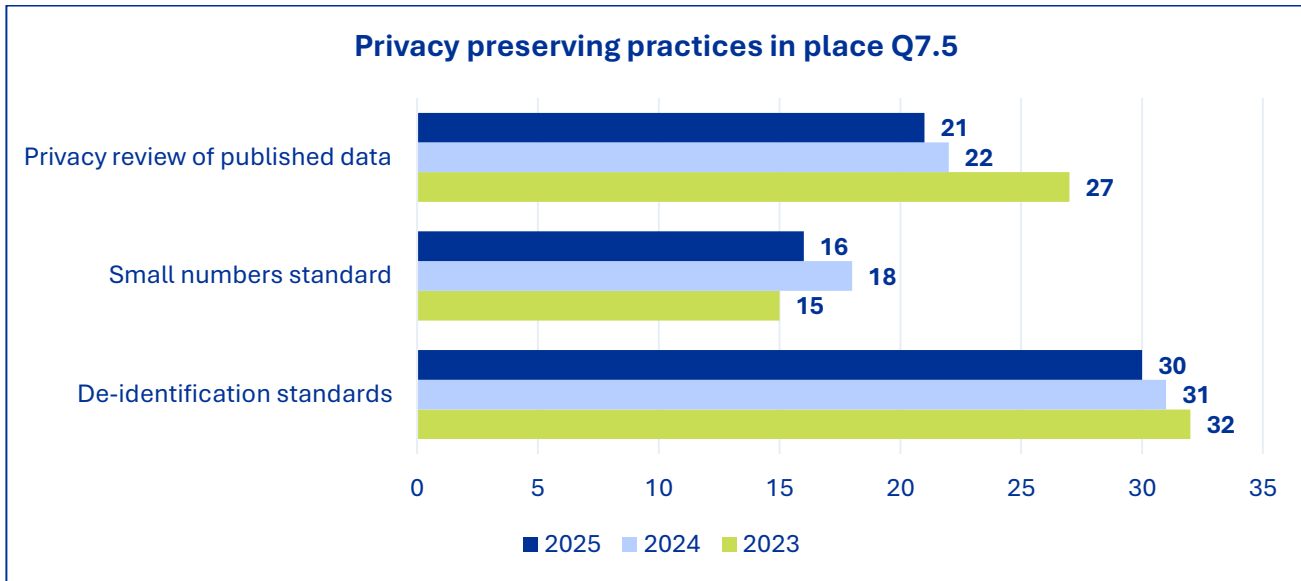
In addition to sharing personal information, agencies disclose information to remain transparent and accountable for government operations. These disclosures include reports to the Legislature, publishing data on websites or open data portals, and sharing analysis with interested parties. Agencies can 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 that can be linked to individuals 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 is small. A “small number standard” sets 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.

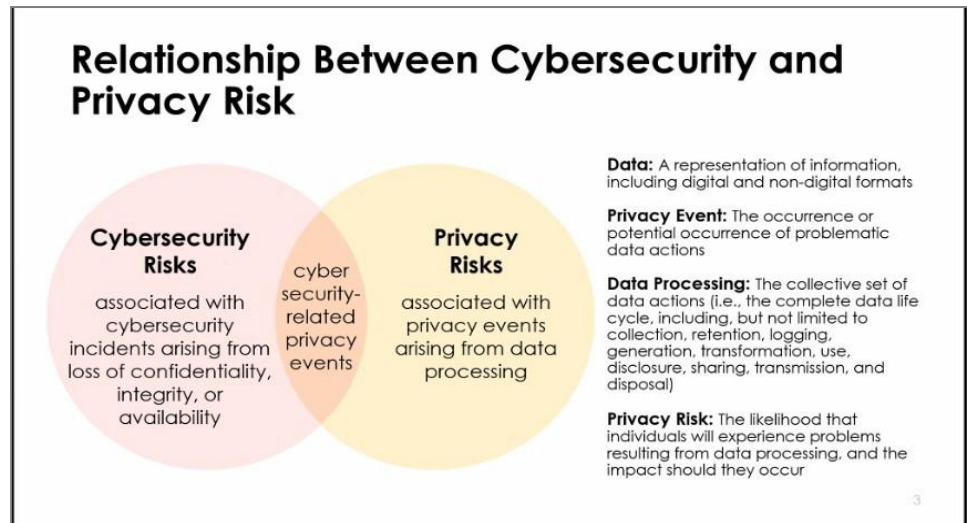


## Data inventory and data deletion

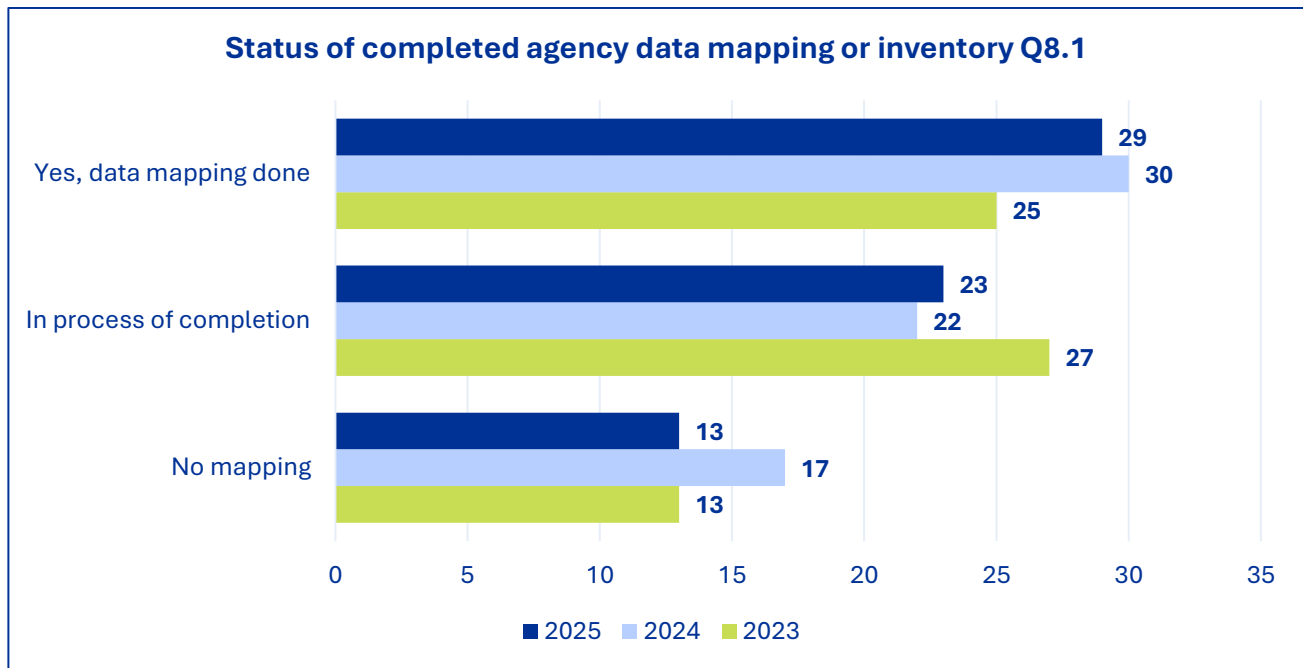
Agencies often collect a variety of information from different sources and maintain it in numerous locations. Understanding what data is maintained and where it is kept is critical to ensuring appropriate data protection measures. Without knowing what information is stored in a specific system, it is 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 demonstrates the relationship between cybersecurity and privacy for data related events due to data processing activities.

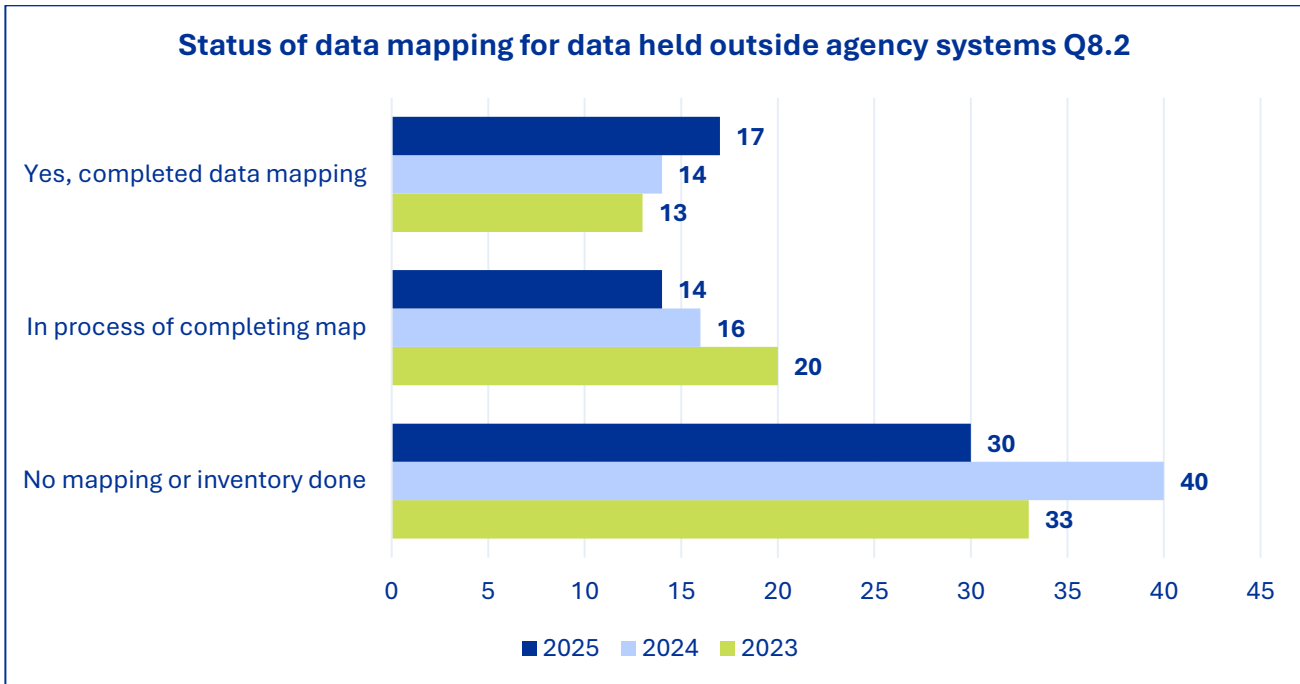
Recognizing that data inventories for data processing activities can be difficult to accomplish, and are often more complex than expected, the OPDP survey asked agencies about mapping data in two places – within agency systems and applications, and outside of agency systems and applications.



The chart for question 8.1 shows a comparison of agencies that have completed data mapping or an inventory of information *within* agency systems and applications. The 2025 data reflect completion of data mapping activities that were underway in the past.



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.

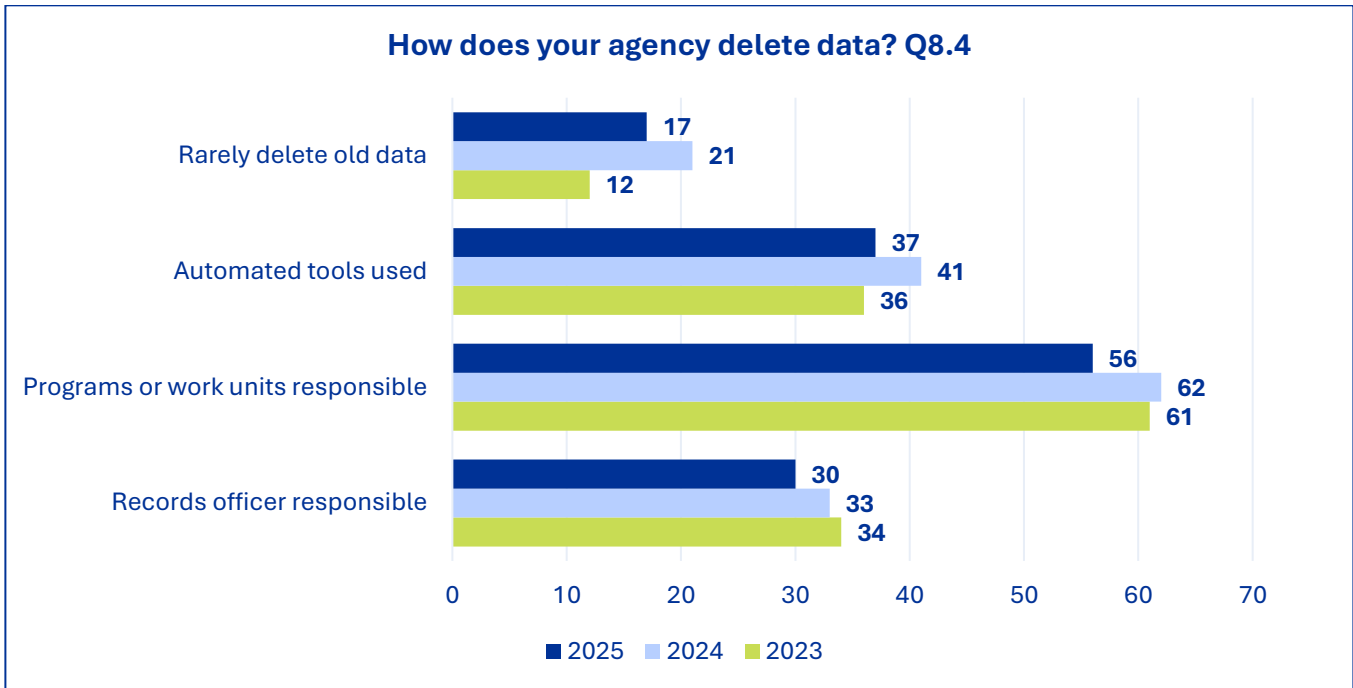


The process of data management and data inventorying offers organizations an opportunity to implement data minimization strategies and delete unneeded data. This process can also lead to cost savings and reduces risk and liability (less data means less cost to store and protect data). In asking agencies 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 2025, across state government:

- 17 agencies rarely delete old data.
- 30 agencies have their records officer delete data.
- 37 agencies use automated tools to delete data.
- 56 agencies have individual work groups or programs responsible for deletion.

*Note: agencies could choose more than one method and so totals add up to more than 67 respondents.*



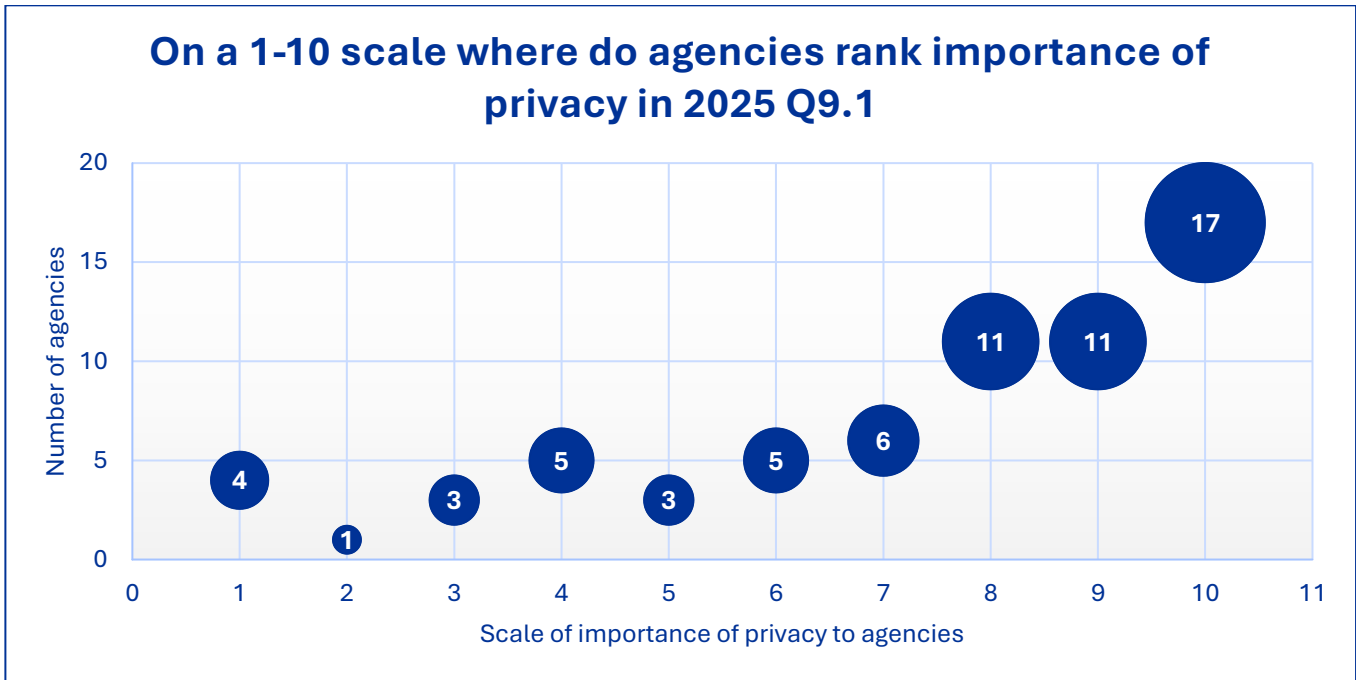
## Future planning

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

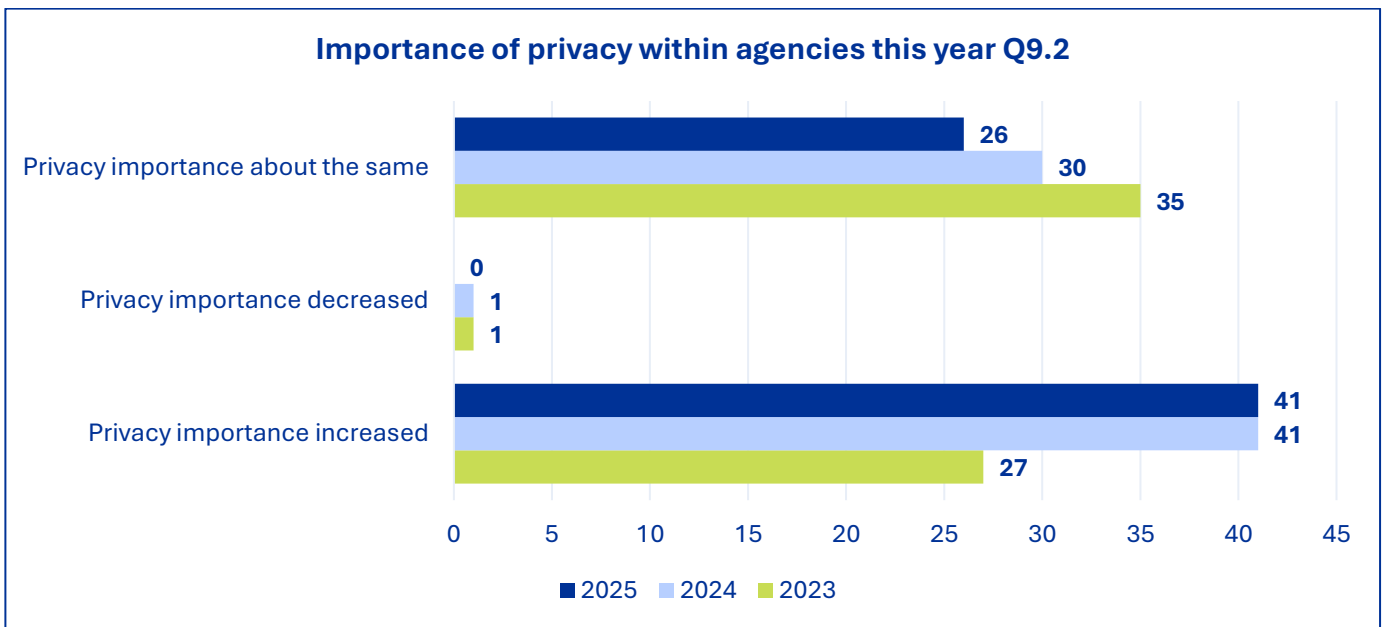
Agencies were asked about the importance of privacy to their agency; what privacy activities they already have planned over the next year; and what additional resources would be most helpful to their privacy posture.

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

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

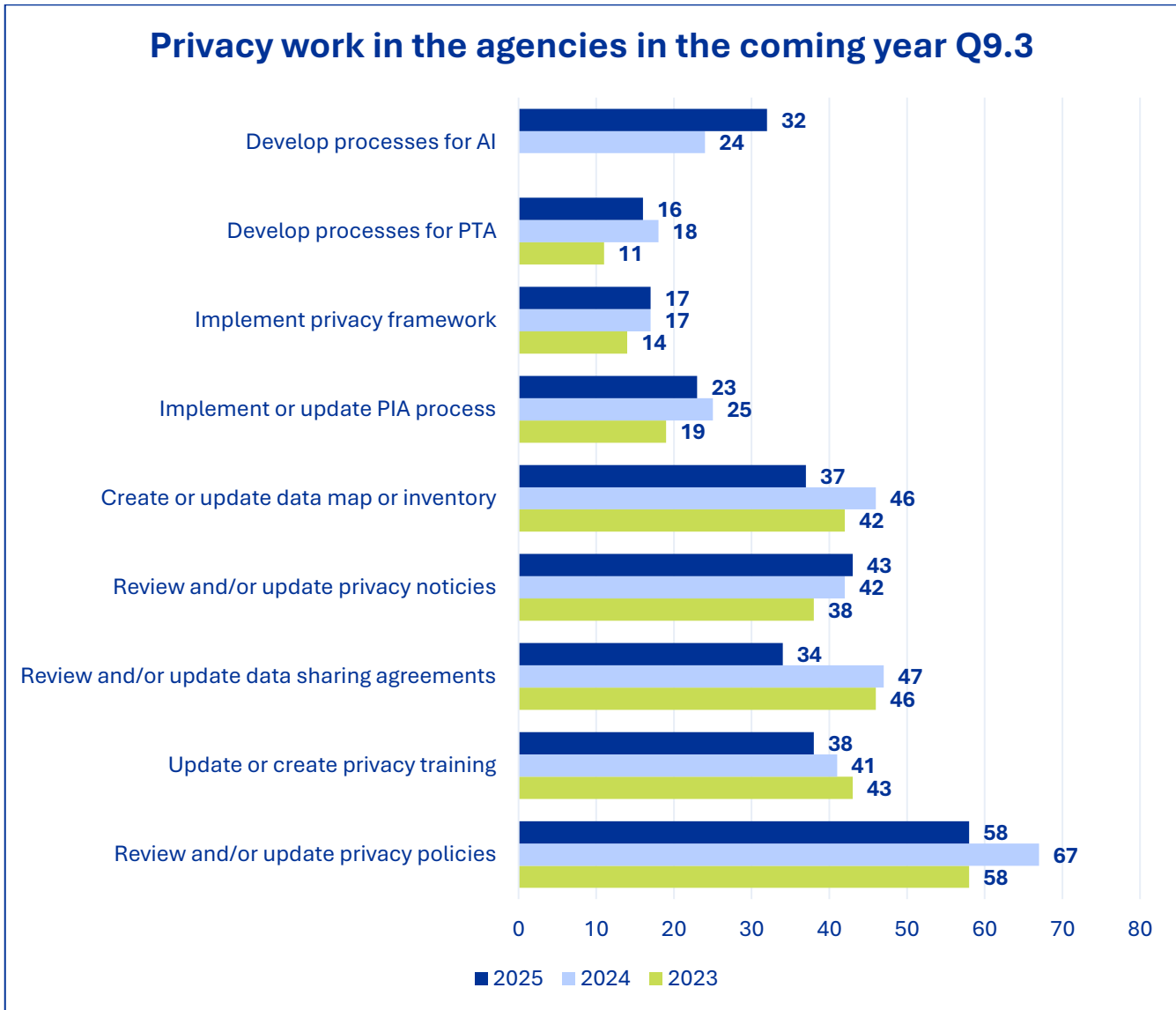


The importance of privacy is confirmed by responses of 67 agencies submitting that the importance of privacy is ongoing or has increased over the last year. Many agencies already have privacy as an ongoing important factor in their work due to long standing state or federal law.



There is an active and diverse set of work planned for 2026 as reported in the 2025 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. OPDP has supported substantial work in AI for the state.



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 over the last four years. It can be found here: [OPDP Performance Report 2024](#). As mentioned previously, the JLARC report also looked at the work of OPDP over the last few years and the report can be found here: [JLARC report on OPDP](#). A JLARC video summation can be found here: [JLARC OPDP video](#).

Please visit our website for more information and resources that our office provides at [Privacy and Data Protection | WaTech](#).

## Contact

For more information or questions about this report, please contact: Katy Ruckle, State Chief Privacy Officer at [privacy@watech.wa.gov](mailto:privacy@watech.wa.gov).