WaTech
Washington Technology Solutions

Office of Privacy and Data Protection Performance Report

December 1, 2024

Table of Contents

Report requirement

The Office of Privacy and Data Protection (OPDP) is required to prepare and submit this performance report to the legislature every four years under RCW 43.105.369(5). The report must include performance measures set in the RCW. These performance measures must include, but are not limited to, the following: (a) The number of state agencies and employees who have participated in the annual privacy training; (b) A report on the extent of the office of privacy and data protection's coordination with international and national experts in the fields of data privacy, data protection, and access equity; (c) A report on the implementation of data protection measures by state agencies attributable in whole or in part to the office of privacy and data protection's coordination of efforts; and (d) A report on consumer education efforts, including but not limited to the number of consumers educated through public outreach efforts, as indicated by how frequently educational documents were accessed, the office of privacy and data protection's participation in outreach events, and inquiries received back from consumers via telephone or other media.

Letter from the State Chief Privacy Officer

I am pleased to present the performance report of WaTech's state Office of Privacy and Data Protection (OPDP). Over the past four years, OPDP has made significant strides in maturing privacy as a discipline. With strong support from the Governor and Legislature, Washington is recognized as a national leader for privacy.

In 2023, I had the honor of being recognized by the Governor for an Outstanding Leadership Award for Washington state and in 2024 I was honored with two national awards for OPDP's work from GovTech and StateScoop. I share this recognition with my stellar team of privacy experts without which our progress would not have been possible. I also want to recognize the hard work by agencies, who have been raising the bar and maturing their privacy programs. This collective work has helped improve privacy maturity across Washington and put in place leading practices to protect personal information.

This report delves into the important work of the state privacy programs, including building on Washington's foundational privacy principles. When I started this position in January 2020, I was the only person in my office and had no budget or staff. Fast-forward to 2024, OPDP now has four employees and has implemented new privacy trainings, developed internal and external government collaboration, and implemented the state's first enterprise privacy policy. Our office also has leveraged funding under the State and Local Cybersecurity Grant program to help agencies and local governments upskill their workforce using professional privacy certification training.

I am proud of our many accomplishments, but there is much work ahead. OPDP is already engaged in multidisciplinary efforts and initiatives to prepare the state for what is next for privacy in the realm of artificial intelligence. Looking ahead we must continue to build upon our foundations as we prepare Washington for the opportunities and challenges presented for the state in emerging technologies.

I look forward to our office's ongoing collaboration with our partners as we continue to lead on privacy and data protection.

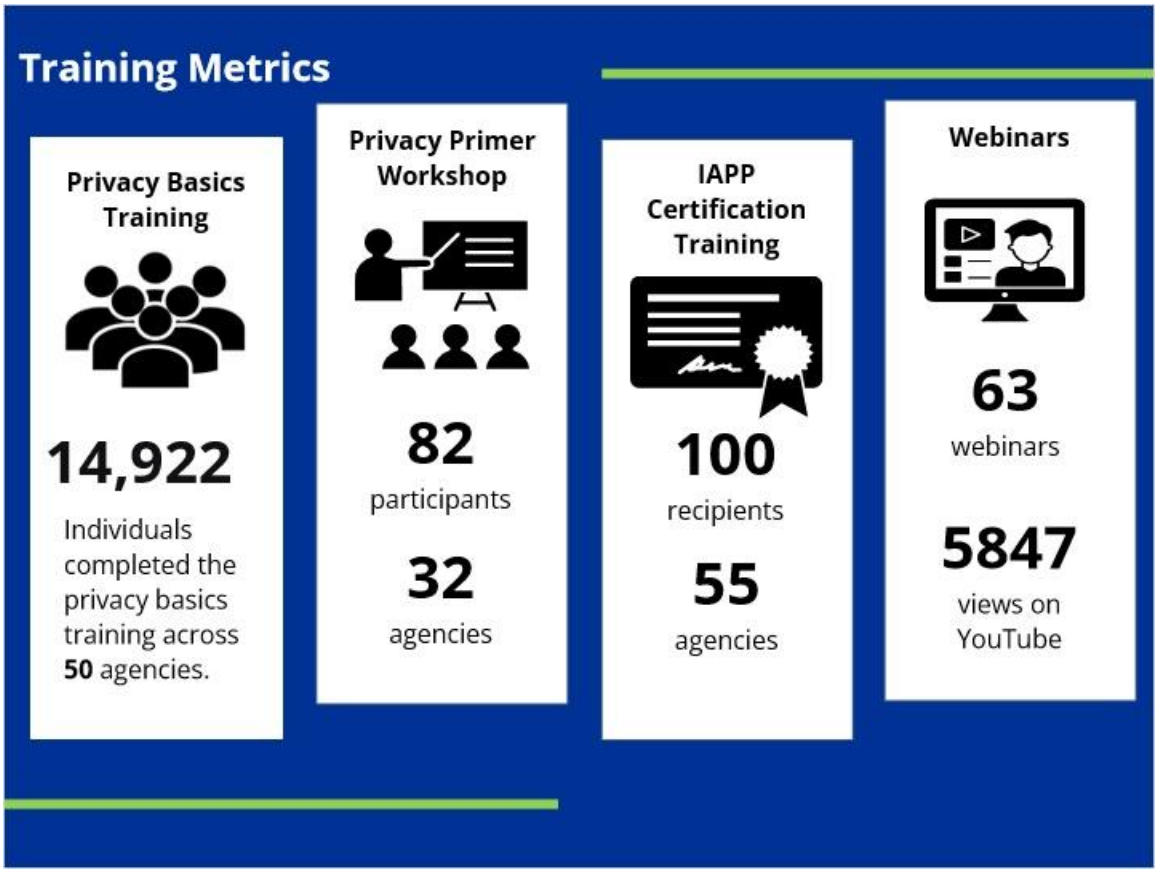
Katy Ruckle

State Chief Privacy Officer

Webinars and trainings

In 2020, OPDP determined the best path towards a scalable enterprise privacy program was to make training and educational initiatives an integral focus. Over the last four years, our office developed various training tools and hosted webinars on a wide range of privacy related topics to effectively reach our audiences. Our webinars and trainings have been attended by people across the state and beyond. OPDP regularly receives inquiries and questions from inside and outside the state about our materials and trainings. Speaking requests for the State Chief Privacy Officer, and her team validate the reach and effectiveness of the trainings and educational materials created for privacy programs.

Here is a breakdown of all the trainings that were offered in the last four years:



Privacy Basics for Washington State Employees – State employees will recognize standard training for such topics as ethics in government, cybersecurity, and safety standards. In 2022 we developed a web-based privacy training to join those well-known trainings that is available to all state agencies through the Department of

Enterprise Services (DES) Learning Center. The training is intended to be a privacy primer for all employees to understand what privacy is, why it's important and how it is distinct from cybersecurity. The course has three parts:

- **Intro to Privacy:** An overview on personal information, data categorization, and privacy harms and violations.
- **Privacy in the State of Washington:** This covers laws and policies, and state agency Privacy Principles.
- **Privacy in Practice:** A deeper dive into agency and employee responsibilities, and privacy best practices.

Since its release, 50 agencies have adopted the Privacy Basics training as their primary privacy awareness training to address how to identify personal information and employee responsibilities for protecting it. Over 14,000 state employees have taken the training through the DES Learning Center platform to date. The training is fully accessible and complies with eLearning standards, ensuring an inclusive and effective learning experience for all participants. We also made the training accessible to everyone to allow greater public access to the information by posting the training on YouTube. The training course has over a thousand views on YouTube which demonstrates the need and interest for the training, beyond the agencies that are currently requiring the training. If you are interested, you can find the training on the OPDP website.

Privacy Primer Workshop – The Privacy Primer Workshop is a formal two-day in-person interactive workshop that provides attendees with information and tools to establish agency privacy programs or to enhance existing programs. Our office developed the curriculum and workshop exercises and activities with external privacy professionals. Over the years we have continued to refine and update the training to keep it topical and fresh. The workshop gives attendees an opportunity to actively participate, collaborate with colleagues on best practices, and participate in group activities that encourage team building and networking while solving privacy related problems. In the two days we cover topics such as:

"Workshop really well done! Loved the energy and enthusiasm for the subject matter!"

-Oct. 2024 Privacy Workshop attendee

"While AI has been discussed a great deal in recent years, the coverage on the topic was fantastic and insightful!"

-Oct. 2024 Privacy Workshop attendee

- Privacy Foundations.
- Business Environment and Privacy Principles.
- Privacy Program Development & Risk Assessment.
- Governance, Policies, Processes, and Technology.
- Trends in privacy and hot topics.
- Action Plan Development.

Since 2022, OPDP has hosted five Privacy Primer Workshops. Four of the sessions were in-person and one was virtual. The virtual workshop was by request for those who couldn't attend in person. Since we began this training, 82 individuals from 32 agencies have participated. Because the web-based training is a prerequisite for these interactive trainings, the collaboration and discussion becomes a key part of the learning for attendees. Participants can dig into the nuances and context of specific agency privacy issues with other professionals.

OPDP provides evaluations on a scale of 1 to 5, with 1 being not satisfied and 5 being very satisfied with the workshop. Our average score over the 5 workshops was 4.8. Here are a few quotes from the evaluations of our most recent workshop in October 2024:

- "Privacy framework and guidelines for building a privacy program were most interesting and useful."
- "The trainers did a great job keeping class energy up – very engaging."
- "Very approachable and competent instructors."

International Association of Privacy Professionals (IAPP) Certification Training Program – In addition to providing grants for cybersecurity, the federal State and Local Cybersecurity Grant Program (SLCGP) also emphasized the overlap with privacy as specified in the federal law. Twice, over the last two years OPDP applied for, and was awarded, grant funding to offer certified privacy training to public employees. Katy Ruckle is the first state Chief Privacy Officer in Washington to earn the IAPP certification and Fellow of Information Privacy distinction. She recognized the benefit to the state and has not only encouraged her small staff to pursue the certification, but also pursued the funding for other public servants at all levels of government.

State and local government employees perform a variety of functions that require handling personal information and public agencies have an obligation to handle information about Washington residents responsibly and in a fair and transparent

way. OPDP recognizes that organizations may lack resources when it comes to privacy training for their staff. With hopes of filling that gap with this funding our office partnered with IAPP to offer industry recognized privacy training and education for public sector employees. Each funding round allows 50 public sector individuals to participate in the training program. The training voucher covers the training class, examination fees and 1-year of IAPP membership for each recipient. Recipients can choose from the following three training certification programs:

- Certified Information Privacy Professional, US (CIPP/US).
- Certified Information Privacy Manager (CIPM).
- Certified Information Privacy Technologist (CIPT).

The training, certification exam, and membership costs $1845.00. Through the funding grant, OPDP was able to make it available at no cost to 100 public employees in both state and local government. The goal of this program is to increase the number of trained and certified privacy professionals in the state and local government workforce. OPDP has received a total of 114 applicants from both rounds of grant funding representing 55 different agencies, highlighting the need and interest in privacy training. This interest is one of the reasons we applied for the grant twice. Increasing trained privacy professionals across every level of government is one of the ways OPDP hopes to leverage our small staff across the entire state to better protect individual's personal information and develop privacy program maturity in government.

Webinars – The Office of Privacy and Data Protection hosts at least 11 educational webinars each year. Seven of those webinars are on privacy related topics, the other four are the State Agency Privacy Forums (SAPF). On average we have 100 public employees from across the state who attend these webinars. Between the SAPF and the regular webinars, OPDP hosted a total of 63 webinars in the last four years.

The State Agency Privacy Forum is held quarterly. This meeting is for public employees with an interest in privacy, or whose work involves privacy. Attendees often include agency privacy professionals, IT workforce and IT security professionals, as well as from areas such as: contracts, risk, legal, legislative, records, and public records professionals. This quarterly meeting is sent out to 132 individuals, with many attending regularly. The advent of remote meetings has increased participation of the state workforce.

"OPDP is a small team doing the work of champions. I really appreciate all the resources and webinars - and how accessible and available they are to agency staff. This is truly good government at its finest."
~Dept. of Commerce

In the 2024 privacy assessment survey, 49 agencies reported that they attended a webinar hosted or created by OPDP in the last year. These webinars are open to anyone in the state government who has an interest in the topics presented. The distribution list for these webinars is continuously growing with new people requesting to be added on a regular basis. Currently the invites go to over 400 individuals across the state enterprise. At the request of state workers who are unable to attend, OPDP also records and posts the webinars on our website along with the slide decks. Currently, we have close to 6,000 views on webinars we previously posted. The top five most popular webinars are:

- Managing personal information & reducing risk with data classification.
- Washington's Data Breach Notification Law for State & Local Government.
- What are Automated Decision Systems and why you should care?
- Webinar on Artificial Intelligence.
- Privacy and Data Protection Policy Webinar.

To access these trainings and more you can visit our Government Agency Resources.

Privacy Threshold Analyses and Privacy Impact Assessments

Privacy assessments are a central piece of effective privacy and data protection programs. More than a best practice, they are required for:

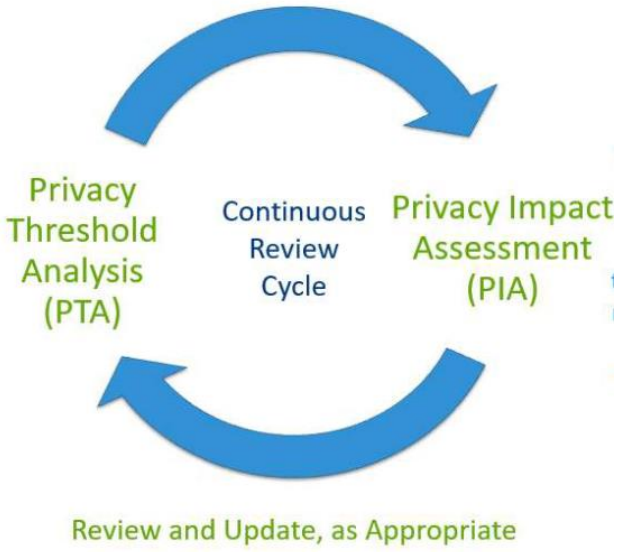
- Federal agencies by the E-Government Act of 2002.
- Public and private sector organizations subject to the General Data Protection Regulation in the European Union.
- Private sector organizations subject to comprehensive privacy laws passed in 17 states across the country since 2018.

Most Washington state agencies did not historically conduct formal privacy reviews. Instead, privacy was often conducted on an ad hoc basis as potential issues were identified. This meant that, even for agencies with dedicated privacy roles, privacy risks could be easily missed, misunderstood, or identified too late. Building processes for formal privacy assessments presented a tremendous opportunity to build out foundational best practices across the enterprise and dramatically expand the role of privacy in projects involving personal information.

OPDP launched a new privacy review process at the end of 2022 and formalized its requirements as part of the enterprise Privacy and Data Protection Policy in June 2024. To date, 40 agencies have participated in this process.

What are PTAs and PIAs?

Privacy assessments are a two-step process. A **Privacy Threshold Analysis (PTA)** is an initial and brief review used to determine whether the project under review may have heightened privacy risks that justify a complete **Privacy Impact Assessment (PIA)**. The PIA is a more in-depth tool used to consider how privacy principles have been incorporated, assess privacy risks, identify how to mitigate those risks, and document all of the above for future monitoring.



Benefits of PTA/PIA process

Key benefits of an established PTA/PIA process include:

- **Creating a formal place for privacy review.** Privacy is a relatively new discipline. Without an established process, it can be difficult to know when or how to conduct a review. A PTA/PIA process ensures there is at least one place for that review to happen.
- **Shifting privacy left.** Without a formal process, privacy is often not considered until a specific issue is identified. This can happen after contracts are signed, after a system and business processes are designed, or even after implementation. The PTA/PIA process moves privacy earlier in the review process to proactively identify risks while there is still time to address them.
- **Better collaboration.** Privacy is inherently multi-disciplinary. The PTA/PIA process helps foster collaboration between business and technical teams, which improves the project.
- **Improved compliance, decreased risks and increased trust.** Overall, performing privacy reviews helps ensure compliance with any applicable laws. They help decrease privacy risks that are unrelated to compliance by improving responsible data processing. And most importantly, they ultimately help improve customer and public trust by demonstrating effective practices and preventing bad outcomes.

PTA/PIA process implementation

New governance processes work best when they are integrated into existing processes rather than built from scratch. Integrating new processes can help reduce redundancy and allows faster implementation.

With that in mind, OPDP worked closely with WaTech's Office of Cybersecurity to integrate a new PTA/PIA process into the well-established Security Design Review (SDR) process. When an agency opens a new SDR, they indicate whether the project involves processing personal information. If it does, a PTA is automatically requested and the SDR will not be closed until the PTA is submitted.

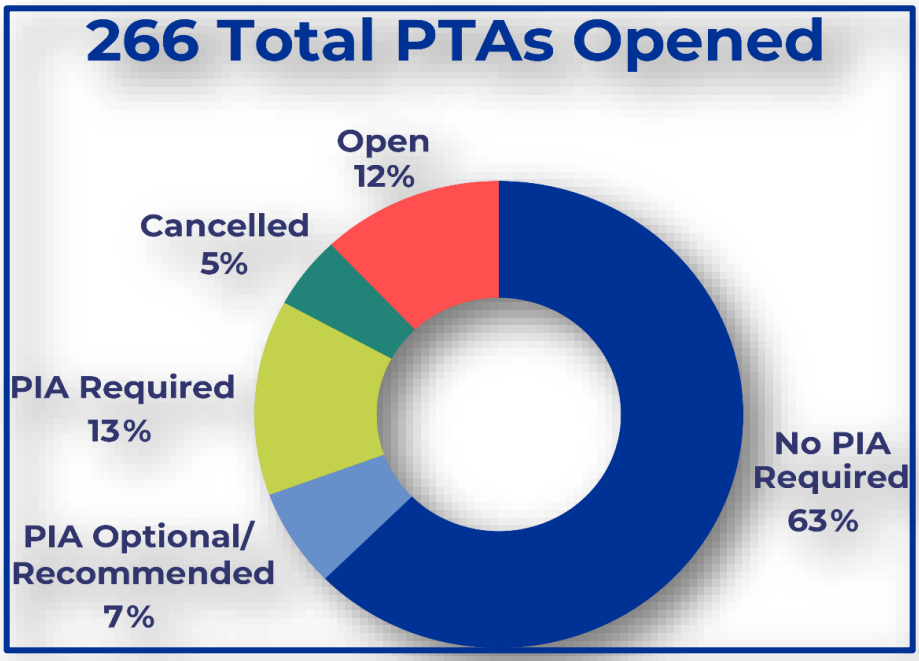
Once an agency submits a PTA, OPDP uses the information to determine if there is a potential for significant privacy risks. That determination considers characteristics about the data, such as type and amount, and the specific uses, such as the type of technology and how information will be shared.

During the implementation period, OPDP conducted extensive outreach to explain the new process and answer questions. These activities included:

- Communicating directly with the privacy community through the Privacy Community of Practice and State Agency Privacy Forum;
- Hosting a webinar and published the materials online;
- Presenting to the Business Management Council and Technology Management Council; and
- Meeting with agencies one-on-one during their first time through the process and as needed for subsequent reviews.

OPDP also routinely meets with OCS to continuously coordinate and improve the integrated process.

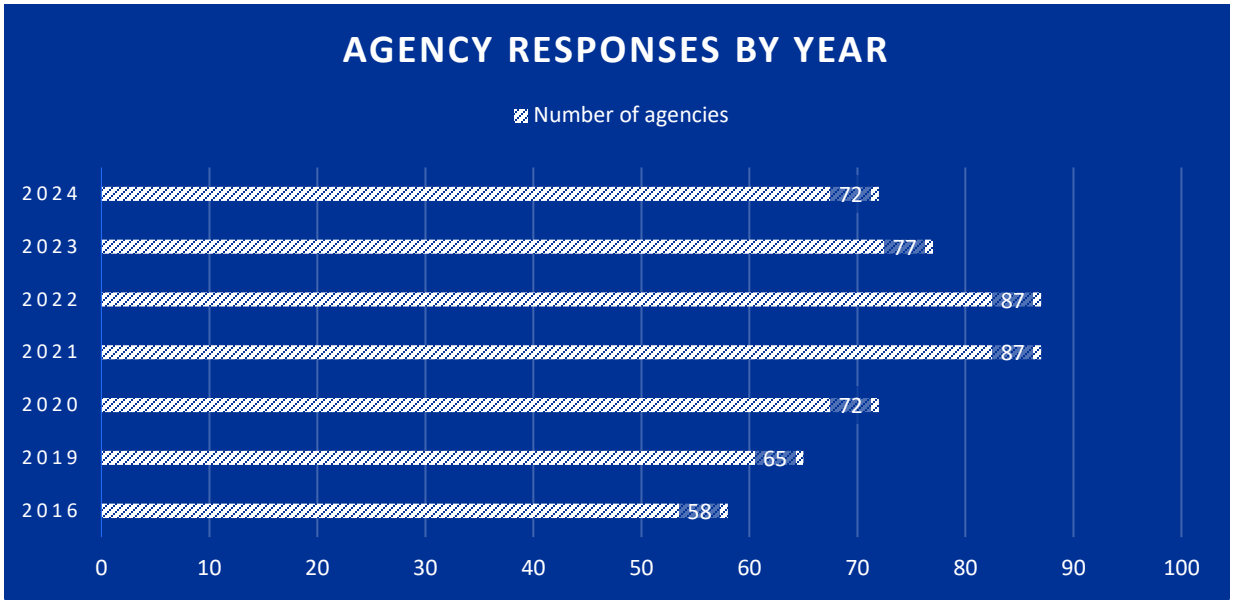
This new work has been immensely successful across the enterprise. As of Oct. 16, 2024, PTAs have been opened for 266 projects across 40 agencies. Of those 266, a PIA was required for 36 projects. Although PIAs are only required for a small fraction of all projects, there are benefits anytime an agency completes a PTA. It provides an opportunity for initial privacy review and often helps identify privacy risks even when those risks don't justify a complete PIA.



Annual state agency privacy reviews

RCW 43.105.369 requires OPDP to conduct an annual privacy review of agency practices. The results help OPDP measure privacy maturity across state agencies and develop resources and trainings where they are most needed. The goal of the annual review is to establish an understanding of current practices. Agency functions and privacy requirements vary. What is a best practice for one agency may not apply to another. The annual privacy survey gives a high-level view of privacy practices across the state.

Since the first assessment in 2016, the number of executive branch agencies that respond to the privacy assessment survey has steadily grown. The State Chief Information Officer now sends the assessment to agencies as part of the 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. The annual privacy survey report offers a more detailed and comprehensive look at the agency responses and year over year changes.

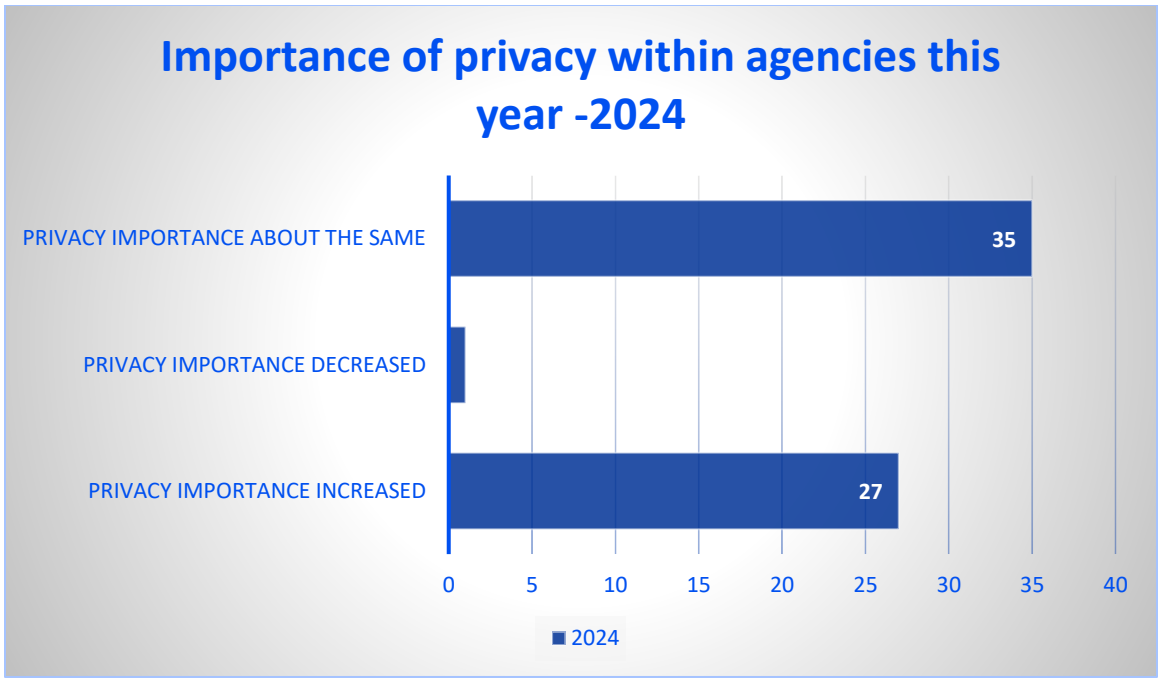
While the assessment helps gather valuable information about agency privacy practices, it is inherently quantitative. For example, it may measure whether an agency has formal policies and staff training but does not evaluate the adequacy of the policies or measure the effectiveness of the training. Data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

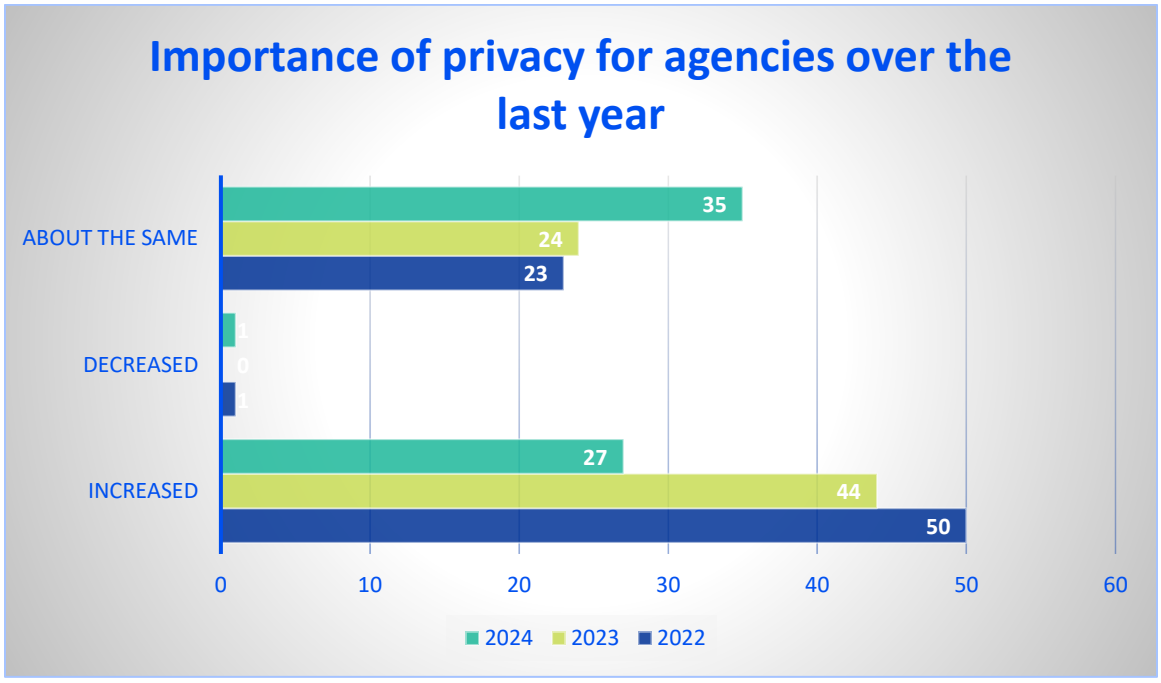
The survey is sent to over 90 state agencies, including some which do not directly report to the executive branch, some agencies which respond through larger supportive agencies, and some which do not hold personally identifiable information. In 2020, 72 agencies responded, compared to 58 agencies in 2016. At the time of this writing in 2024, more than 80 agencies responded to the 2024 survey with some agencies still in the process of submittal. The variance in responses is attributable to changes in personnel, agency organization, and voluntary participation from higher education institutions and other branches of government. Due to these factors, it is not expected that every single agency will respond to the assessment survey.

The survey questions have remained similar year over year for data comparison. Some questions have been added over time as needed to gather information on new topics (such as metric use, or Artificial Intelligence use) or removed due to obsolescence.

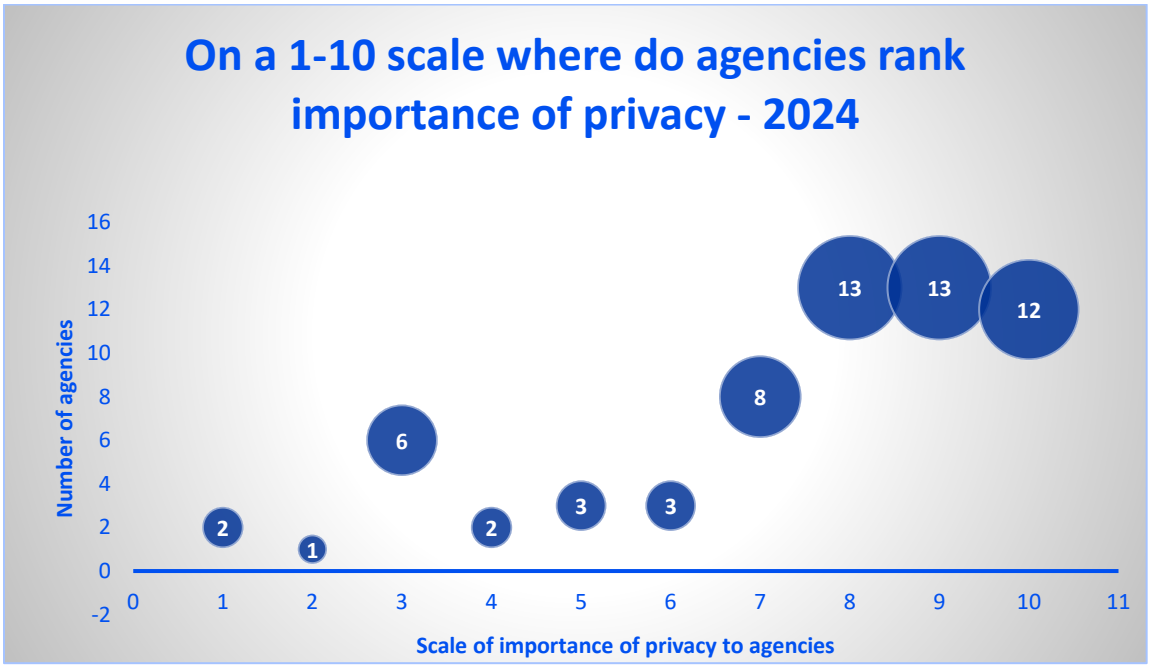
In 2024, 63 agencies reported they maintain personal information and indicated that privacy is a significant priority. Only one agency indicated privacy had decreased

over the last year. (Of note: agencies that are responsive to the federal health care law, Health Insurance Portability and Accountability Act – HIPAA, usually have more mature privacy programs.) All other agencies reported that the importance of strong privacy controls had increased over the last biennium (35 agencies) or stayed the same (27 agencies). After rapid changes in the privacy area, this is consistent with greater implementation and awareness of privacy policies and guidelines.

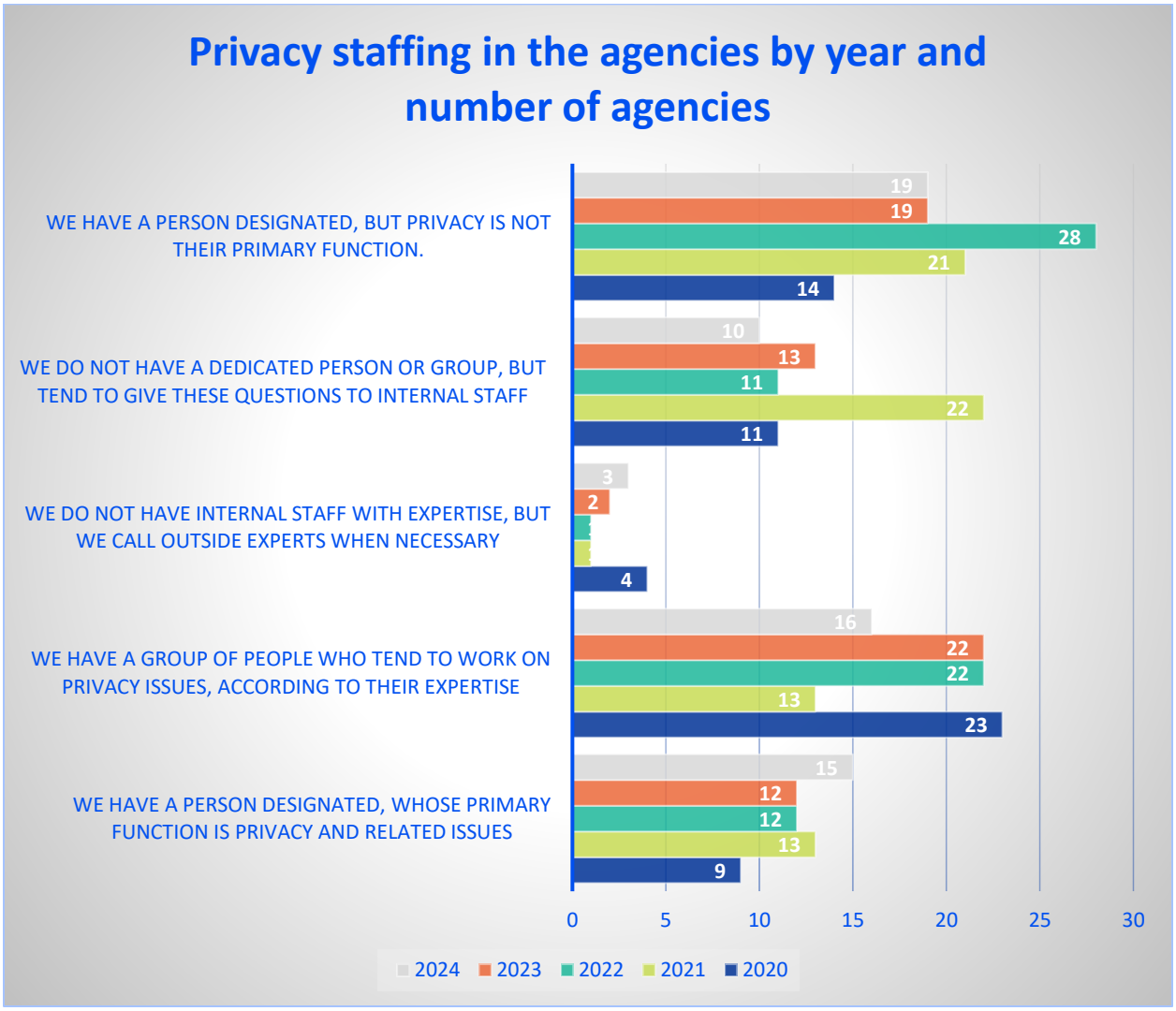




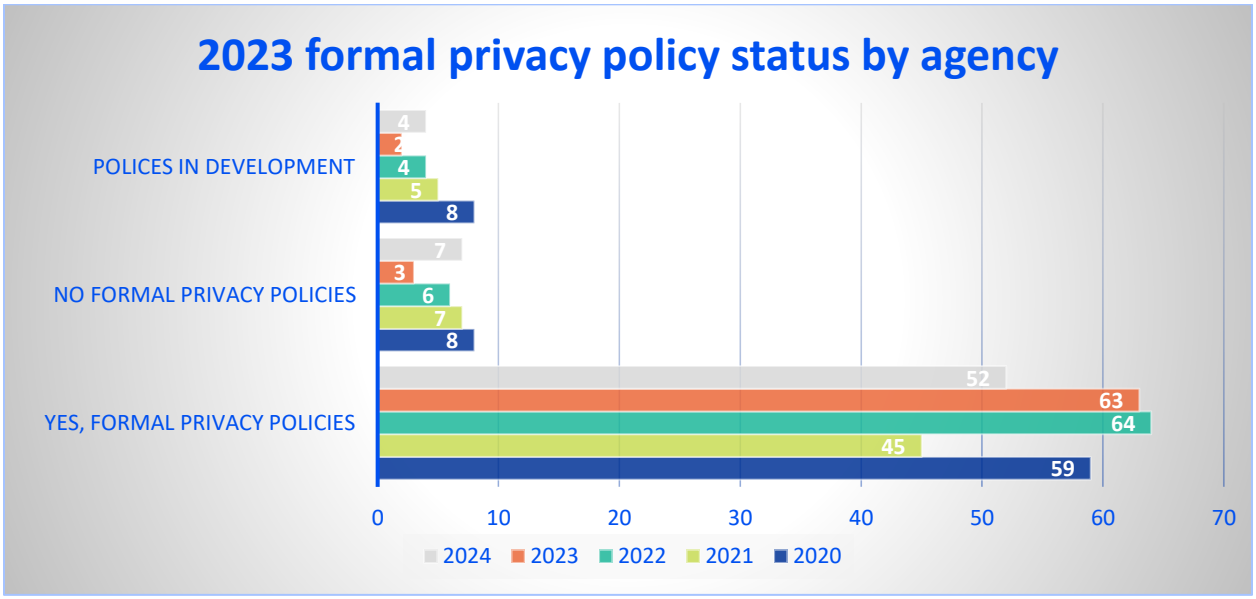
Agency recognition of the importance of privacy is well founded given public attitudes towards the government's use of data, and the types of personal information agencies maintain. Agencies often collect information that goes far beyond names and contact information. For example, this year 47 agencies reported collecting social security numbers, 43 collect demographics information, 37 collect medical information and 29 collect immigration or citizenship information. Within this context, the importance of privacy across agencies is consistent with what kind of data and how much data agencies steward. (The annual privacy survey report dives deeper into the types of personal information agencies maintain and who the agencies share that data with.)



Responses confirm agencies are taking steps to protect personal information. Staffing is a key component to a robust privacy program and is part of that protection effort. Agencies continue to designate a person or group to deal with privacy issues. For the first time in five years, there are more staff in agencies, specifically designated to deal with the increasing complexity of privacy laws.



Another key component of privacy programs are policies. A majority of agencies have consistently maintained formal internal privacy policies. Agencies have also consistently updated and developed privacy policies over the last four years.



Even with this progress, the assessment continues to reveal opportunities for improvement by agencies and OPDP. As awareness and concern about privacy continues to increase, many agencies are looking to improve their privacy practices. The level of maturity varies. Some are developing practices for the first time while others are turning privacy policies into privacy programs or are expanding existing privacy programs.

More agencies than ever are utilizing resources and trainings from OPDP as their privacy programs grow. In 2024, over 50 agencies were aware of the training developed by OPDP, and 38 agencies responded that they use the training developed by OPDP. In 2024, 49 agencies reported that they had attended a webinar hosted or created by OPDP. One of the most exciting pieces of data from the 2024 survey was seeing that every agency that responded had utilized at least one resource from OPDP – data breach assessments, and data share templates being two of the most used resources created by OPDP.

All agencies are looking for guidance and assistance. Dedicating resources that allow the OPDP to conduct additional outreach and create additional resources will fill an identified gap for WaTech customers and help ensure appropriate best practices to protect Washington residents' information.

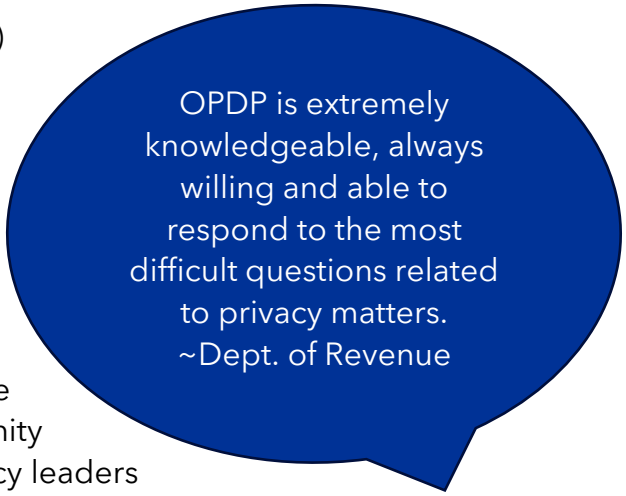
Overall, OPDP found that agencies are more likely to have core privacy program components – such as dedicated staff and formal policies and trainings than in the past. However, gaps remain and even agencies with more privacy experience consistently indicate they need additional resources. This need will 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. These principles were finalized in October 2020 and the privacy survey is largely based on that framework.

The annual privacy survey offers both an excellent high-level snapshot of privacy at the enterprise level, as well as educated opportunities to focus limited privacy resources within state government.

External collaboration and leadership

The Office of Privacy and Data Protection (OPDP) plays a pivotal role in managing and fostering relationships with governmental entities, regulatory agencies, and other external partners concerning privacy and data protection issues. Our government relations and collaboration efforts are focused on several key objectives:



- **Enterprise privacy policy leadership**: We actively engaged with the privacy community and agency technology and business policy leaders to create Washington's first enterprise privacy policy. This included creating the policy with privacy professionals' input and collaborating with agencies to adopt Washington's privacy principles.
- **Incident management and response**: OPDP serves as the primary liaison between our organization and the Office of Cybersecurity on major incidents that affect privacy. We ensure that our compliance efforts align with the Enterprise Incident Response Plan and open communication and coordination with agencies to address multistate-agency incident response.
- **External partner engagement**: We maintain relationships with relevant partners, including national organizations, industry associations, privacy advocates, local governments and academic institutions. By participating in forums and conferences, we contribute to the broader discourse on privacy issues and gather insights that inform our practices. Our team members are sought after conference speakers and regularly present on privacy issues.
- **Monitoring legislation and trends**: Our team continuously monitors changes in privacy legislation and emerging trends in data protection. This proactive

approach enables us to anticipate regulatory shifts and keep state agencies up to date on potential impacts.

- **Public education and awareness**: We work collaboratively with government entities to promote public awareness of privacy rights and responsibilities. Through educational initiatives and outreach, we aim to enhance understanding of privacy issues. As the State's Chief Privacy Officer, Katy Ruckle writes and distributes the monthly newsletter *Privacy Points* and annually we celebrate international data privacy day every January.

By effectively managing external collaboration, the Office of Privacy and Data Protection provides leadership to ensure that our agencies not only comply with applicable laws, but also leads in responsible and ethical data handling practices, which fosters public trust.

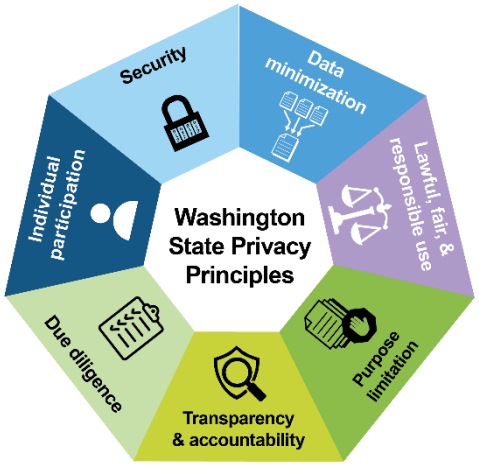
Enterprise Policy and Leadership

After laying the groundwork for several years on privacy program initiatives and best practices, OPDP was able to implement a comprehensive privacy policy for the state of Washington. The privacy policy included several key areas of privacy programs for state agencies. Below you can see the 14 sections of the Enterprise Privacy and Data Protection Policy. The policy requirements apply to all state agencies subject to WaTech's policies and was approved by the Technical Services Board in June 2024.

Policy Requirements

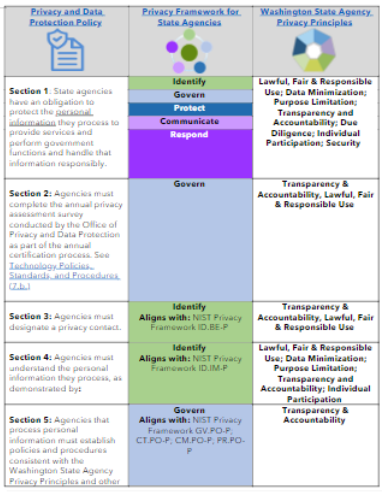
Section		Section	
1	Statement of agency responsibility	8	Data sharing agreements
2	Annual privacy assessment	9	Data disposal
3	Privacy contacts	10	Privacy notices
4	Data discovery and documentation	11	Individual participation
5	Policies and procedures	12	Incident response
6	Privacy impact assessments	13	Monitoring and periodic review
7	Training and awareness	14	Biometrics

One of the most important aspects for successful policy approval and adoption was preparing the agencies over the past several years to have most of these policy sections already in place. By providing resources and building good practices among the agencies, the policy compliance and adoption was less of a lift for agencies to be successful.



For example, agencies were already meeting several of the policy requirements and incorporating the Washington State Agency Privacy Principles that were articulated in 2020. Through this work and the additional resources, OPDP provided the foundation and assistance to help agencies be successful. While some of the adoption work is ongoing, OPDP has provided additional training and implementation materials for successful policy adherence.

In February 2024, OPDP held a training to introduce the enterprise privacy policy to state agencies. In July 2024, OPDP released the Privacy Notice Implementation Guide and an example privacy policy. We also hosted a webinar in August 2024 to train agencies on the policy and best practices for creating a clear privacy notice to help agencies be transparent about how they are collecting and using Washington residents personal information.

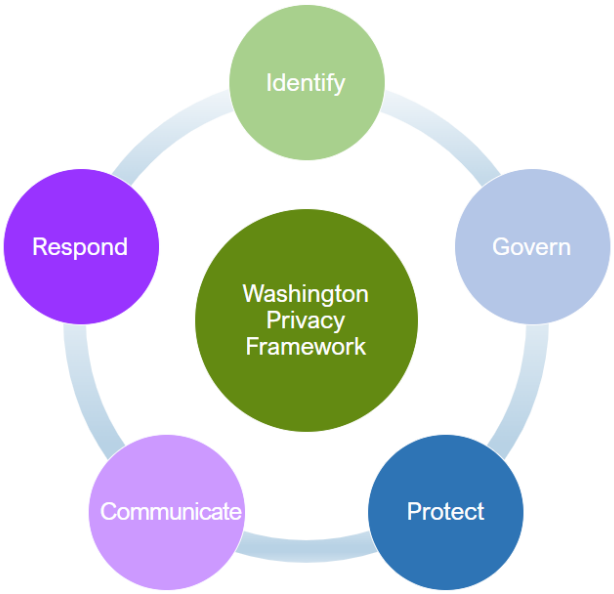


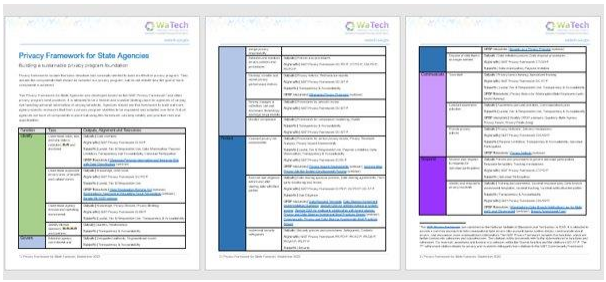
Privacy and Data Protection Policy	Privacy Framework for State Agencies	Washington State Agency Privacy Principles
Section 1: State agencies have an obligation to protect the personal information they process to provide services and perform government functions and handle that information responsibly.	Identify Govern Protect Communicate Respond	Lawful, Fair & Responsible Use; Data Minimization; Purpose Limitation; Transparency and Accountability; Due Diligence; Individual Participation; Security
Section 2: Agencies must complete the annual privacy assessment survey conducted by the Office of Privacy and Data Protection as part of the annual certification process. See Technology Policies, Standards, and Procedures (7.1c.)	Govern	Transparency & Accountability, Lawful, Fair & Responsible Use
Section 3: Agencies must designate a privacy contact.	Identify **Aligns with:** NIST Privacy Framework ID.BE-P	Transparency & Accountability, Lawful, Fair & Responsible Use
Section 4: Agencies must understand the personal information they process, as demonstrated by:	Identify **Aligns with:** NIST Privacy Framework ID.IM-P	Lawful, Fair & Responsible Use; Data Minimization; Purpose Limitation; Transparency and Accountability; Individual Participation
Section 5: Agencies that process personal information must establish policies and procedures consistent with the Washington State Agency Privacy Principles and other	Govern **Aligns with:** NIST Privacy Framework GV.PO-P, CT.PO-P, CM.PO-P, PR.PO-P	Transparency & Accountability

Crosswalk of Privacy Policy to Principles and Privacy Framework

Another resource OPDP created was the crosswalk document to demonstrate how the enterprise privacy and data protection policy incorporates the Washington State Agency Privacy Principles and Privacy Framework.

Our office released the Washington Privacy Framework in 2022. This framework is based on the National Institute Standards and Technology (NIST) Privacy Framework 1.0. While we encourage agencies to use the NIST Privacy Framework as a resource, we learned that it can be overwhelming and intimidating for agencies starting to build their privacy programs. As such we created the Washington Privacy Framework to help agencies understand what should be in place for an agency privacy program.



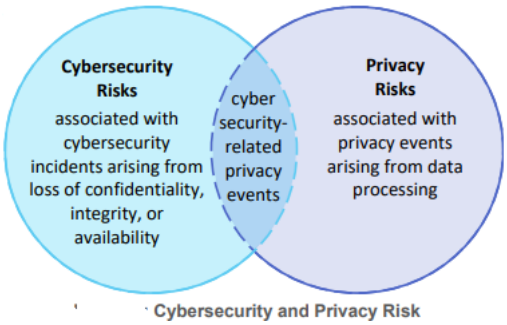


Washington Privacy Framework Document

The privacy framework is intended to be a flexible and scalable starting place for agencies of varying size handling personal information ranging in 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 components in place but using the framework can help agencies identify and prioritize risks and opportunities. The Washington Privacy Framework includes the basic structure and concepts needed to build an effective privacy program and includes the components of a program, but do not dictate how each component is achieved. Later this year we plan to release a web-based training of the Washington Privacy Framework that can help agencies understand the basics of implementation.

Incident management and response

A key area of privacy and security overlap is in the coordination and response to breach incidents. Fortunately, large enterprise incidents are rare, but to competently respond to enterprise incidents the Office of Privacy and Data Protection and the Office of Cybersecurity (OCS) must be in lockstep. Our office worked closely with OCS to draft the Enterprise Incident Response Plan required under RCW 43.105.450. The NIST Privacy Framework demonstrates the overlap between cybersecurity and privacy when incidents occur that may result in the compromise of personal information. OPDP coordinates closely with Office of Cybersecurity and cybersecurity and privacy professionals in other agencies in statewide incidents occur. This work helps to provide consistent messaging to the public when more than one agency is involved.



Cybersecurity and Privacy Risk

External partner engagement

As a part of its statutory responsibility the Office of Privacy and Data Protection regularly engages with national and international experts in the fields of data privacy, data protection and access equity. These organizations include:

- National Governor's Association (NGA).
- National Conference of State Legislators (NSCL).
- National Association State Chief Information Officers (NASCIO).
- National Institute of Cybersecurity Education (NICE).
- Information Professional Managers Association (IPMA).
- Association of County and City Information Systems (ACCIS).
- Washington Association of County Officials (WACO).
- Washington Association of Public Utilities District Association (WAPUDA).
- International Association of Privacy Professionals (IAPP).
- Identity Theft Resource Center (ITRC).
- Privacy & Security Academy at George Washington University.

As for access equity over the course of the last four years our office was involved in the Digital Equity Forum at the Department of Commerce and worked closely with the American Civil Liberties Union (ACLU) on the Automated Decisions Systems Workgroup. In addition, OPDP co-chaired the System Technology and Data Security Subcommittee with the Washington Technology Industry Association (WTIA) for the Washington State Autonomous Vehicle Workgroup.

"I find the work of the OPDP essential for my organization to be able to stay abreast of information about privacy considerations, proposed and enacted legislation, compliance changes, the changing landscape of generative AI, and a host of other important developments. I find the information from quarterly webinars, OPDP website, and other resources very useful as I continue to develop our organization's privacy program." ~Central Washington University

The Automated Decision-making Systems (ADS) Workgroup was prescribed by the Legislature via a budget proviso in the 2021-2023 biennial operating budget. The ADS Workgroup brought together advocacy groups, government agencies, research, and academic experts to "examine how automated decision-making systems can best be reviewed before adoption and while in operation and be periodically audited to ensure that such systems are fair, transparent, accountable and do not improperly advantage or disadvantage Washington residents." Given the breadth and complexity of the work assigned, the workgroup elected to meet every other week and held a total of 10 public two-hour meetings. The work and recommendations of the workgroup culminated in a 44-page report. Although ADS was a precursor to the broader artificial intelligence conversations the state is having today, I am proud of the work that that the workgroup accomplished and its recommendations. Many of our findings and recommendations overlap with what we are seeing nationwide with executive orders in states around AI adoption considerations. These include concepts like system review, procurement, risk, transparency, training, and ongoing monitoring. Additional deliverables that came from this were the ADS inventory and procurement and use guidance as directed by the Governor. All of which is available on the WaTech website.

Monitoring Legislation and Trends

Every year the Office of Privacy and Data Protection follows the legislative session very closely for bills that impact privacy or are in the realm of privacy adjacent activities. Last legislative session we tracked 70 bills, with 23 passing. This is an important service that we can provide to the state agency and local government privacy community so that they can understand what is important to law makers and what to be prepared for when new laws are passed. We usually break down the bills by topics like privacy rights and protection bills, election laws, public records, employee information, law enforcement, and technology bills. OPDP presents to the Technology Services Board on our tracking and monitoring, as well as presenting to internal governance groups like the Technology Management Council and Business Management Council. Additionally, the State Chief Privacy Officer has also presented or testified at the legislature on privacy bills or participated in work sessions in both the House and Senate on privacy.

Public Education and Awareness

After starting as the State Chief Privacy Officer, Katy Ruckle began publishing a newsletter called Privacy Points. Since December 2020, she has published more than 50 newsletters online and distributed through Gov Delivery. OPDP's total number of subscribers has increased 308% since December 2020 from (171 to 697). And the average open rate is 29%, which is higher than the median open rate of 21.5%. The Privacy Points newsletter provides timely information about what our office is working on, new educational materials and resources and promotes upcoming trainings and webinars. Ruckle also touches on some of the privacy trends and legislation OPDP is following. Anyone with an interest can subscribe by selecting the "Privacy Community" at WaTech.

"OPDP has played a pivotal role in safeguarding the data privacy of our state's residents during a period of rapid technological advancement. As technology continues to evolve at an unprecedented pace, OPDP has been instrumental in ensuring that the privacy rights of individuals are protected."
~Employment Security Dept.

Another important event for OPDP every year is celebrating International Data Privacy Day, which falls on Jan. 28. We put together a slate of activities and webinars during that week and work with the Governor's office and legislative members to promote it.


The State of Washington

Proclamation

WHEREAS, Privacy is a foundational right of individuals proclaimed, protected and enshrined in the Washington State Constitution in Article I section 7; and

WHEREAS, a day is set aside each year to recognize the importance of data privacy and data protection on January 28th to raise awareness and promote privacy and data protection best practices; and

WHEREAS, is observed across the world in over 50 countries, in order to draw attention to best practices and innovative discussions that promote individual control over personally identifiable information, responsible privacy practices and compliance with privacy laws and regulations; and

WHEREAS, the Council of Europe first recognized Data Privacy Day in 2007, and the US Congress followed suit in 2009 by passing House Resolution 31 by a vote of 402-0 declaring 28 January National Data Privacy Day; and

WHEREAS, Data Privacy Day is recognized as an educational initiative focused on raising awareness among businesses, governments, and individuals about the importance of respecting individual privacy and protecting personal information; and

WHEREAS, many states, including Washington, have passed or continue to discuss further protecting consumers personal information through education, enforcement and enunciation of the rights of access, correction, deletion, and portability of their personal information; and

WHEREAS, the pervasive use of data collecting and generating technologies in our homes, in our everyday life activities, in schools, and in our work, gives rise to the potential compromise of personal privacy if appropriate care is not taken to protect personal information; and

WHEREAS, The protection of all forms of personal information is a global imperative for governments, industry, civil society, and individuals; and

WHEREAS, the recognition of Data Privacy Day will encourage more people in Washington to become aware of personal information privacy concerns and to take steps to protect their own privacy interests as well as their personal information;

NOW, THEREFORE, I, Jay Inslee, Governor of the state of Washington, do hereby proclaim January 28, 2022, as

Data Privacy Day

I encourage all people in our state to join me in this special observance.

Signed this 11th, day of January, 2022

Last year OPDP focused on children's privacy and discussed policy initiatives with Washington lawmakers, online privacy experts, and the sponsor of California's Age-Appropriate Design Code Act. In the previous year we focused on health privacy and collaborated with the Office of the Attorney General to discuss the annual data breach report. This educational awareness campaign is well attended every year and an important way to raise awareness about our office and the importance of privacy for Washingtonians.

Looking to the future

As we continue to navigate the evolving landscape of data privacy, the Office of Privacy and Data Protection (OPDP) remains an active and engaged office and resource for Washington. The office has made significant strides in enhancing privacy policies and practices. However, the future demands that the state remain vigilant and proactive. The rapid pace of technological advancement presents both opportunities and challenges in how we protect personal information. As Washington's Chief Privacy Officer, I am committed to ensuring that our office remains at the forefront of these developments. Areas of particular importance include:

- **Emerging Technologies:** The rise of artificial intelligence (AI) brings new complexities to data privacy. We are honored to be helping to lead WaTech's work on AI. Through several initiatives like the AI Community of Practice, the Governor's Executive Order on AI, and the AGO AI Task Force we are working to create policies and risk processes to ensure that these new tools can be used responsibly and safeguard individual rights.
- **Regulatory Landscape**: Privacy regulations continue to develop as we understand more about how technology and data collection works. Our office will stay informed about upcoming changes and help the state adopt policies accordingly to ensure compliance and build trust with the public and our employees.
- **Data Minimization**: As we collect and analyze more data, we must prioritize data minimization practices. This means collecting only what is necessary and ensuring that data retention policies are followed.
- **Transparency and Communication**: Open communication with others is essential. We will continue to provide resources and guidance that adhere to the state's privacy principles to be clear about how we collect, use, and protect data, fostering a culture of transparency.
- **Employee Training and Awareness**: OPDP will continue to invest in being a resource for state agencies. Ongoing training will empower our teams to recognize and address privacy issues, making each of us a champion for data protection.

As we move forward, OPDP plans to keep the mindset of continuous improvement as we mature our privacy programs and data initiatives in the state. This is key as we embrace new technologies and modernizing the way we serve our residents.

Together, we can create a privacy-conscious culture that not only meets regulatory requirements but also honors and enhances public trust.

Contact

Katy Ruckle, State Chief Privacy Officer

Washington Technology Solutions

Office of Privacy and Data Protection

Email: privacy@watech.wa.gov

Questions regarding the Office of Privacy and Data Protection Performance Report can be directed to privacy@watech.wa.gov.

Feedback

In the 2024 Privacy Assessment Survey, OPDP asked agencies if they would like to offer quotes about OPDP, resources available to agencies, or the importance of privacy. We received the following quotes:

Dept. of Commerce	OPDP is a small team doing the work of champions. I really appreciate all the resources and webinars - and how accessible and available they are to agency staff. This is truly good government at its finest.
Central Washington University	I find the work of the OPDP essential for my organization to be able to stay abreast of information about privacy considerations, proposed and enacted legislation, compliance changes, the changing landscape of generative AI, and a host of other important developments. I find the information from quarterly webinars, OPDP website, and other resources very useful as I continue to develop our organization's privacy program.
Dept. of Licensing	AI is becoming either transformative or pernicious for our data and privacy work; it's been great to see OPDP representing agencies in state and public fora on this topic.
Dept. of Revenue	OPDP is extremely knowledgeable, always willing and able to respond to the most difficult questions related to privacy matters.
Employment Security Department	OPDP has played a pivotal role in safeguarding the data privacy of our state's residents during a period of rapid technological advancement. As technology continues to evolve at an unprecedented pace, OPDP has been instrumental in ensuring that the privacy rights of individuals are protected. |
Evergreen State College	I feel that the OPDP has done an excellent job of improving the privacy of all Washingtonians over the last 4 years! As a citizen, I appreciate that OPDP is at the forefront of developing best practices and standards that serve as guardrails to our government and prevent oversteps and abuses of power. As an agency representative, I appreciate the resources to help keep us aware and vigilant of protecting the privacy of everyone who entrusts us with their personal information. Thank you for putting together all of the resources that we have available to us.
Gambling Commission	Every Washingtonian has the right to privacy.
Office of Superintendent of Public Instruction	The importance of children's privacy has never been more critical. As students increasingly engage with online learning platforms, social media, gaming, and numerous apps, vast amounts of personal data are collected, stored, and sold\shared. Protecting this sensitive information is paramount to ensuring our children's safety, security, and well-being. With the rise in cyber threats and non-stop data breaches, it is essential that schools, parents, vendors, and policymakers prioritize robust privacy protections to safeguard children's digital identities to foster a safe and secure environment for learning and development.
Puget Sound Partnership and RCO	OPDP is very organized and systematic in offering assistance, tools, and training to agencies.
Health Care Authority	Educating people about their data and how it is used will become more important as AI becomes commonplace. Washington has a long way to go in both educating its citizens and empowering its citizens with laws over how their data can be used. Until one is passed federally, Washington needs a comprehensive privacy act with rights equivalent to those enjoyed in California, Colorado, Virginia, and the European Union.