

# 2022 Privacy Assessment Survey Guidance Document

August 2022  
Office of Privacy and Data Protection

## Table of Contents

Introduction.....	2
RCW 43.105.369 .....	2
Office of Privacy and Data protection. ....	2
Privacy Assessment Survey Sections.....	2
Survey Introduction and Disclosure Cover Page .....	3
Agency Information.....	4
Survey Questions .....	6
1. Types of Personal Information .....	6
2. Privacy Roles and Staffing.....	8
3. Trainings and Policies.....	11
4. Transparency.....	13
5. Individual Participation.....	15
6. Accountability.....	16
7. Data Sharing, Third Party Management, and Data Publishing.....	19
8. Data Inventory, Retention, and Destruction .....	22
9. Future Planning .....	23
Conclusion.....	26

## Introduction

The Office of Privacy and Data Protection is required to conduct an annual privacy review under [RCW 43.105.369](#). This review provides policymakers with a valuable snapshot and metrics of practices, progress, and risks regarding the use and protection of personal information entrusted to state agencies by Washingtonians.

This document can be used to help gather responses to the 2022 Privacy Assessment Survey, which is conducted with the FormStack survey tool. The survey contains a screening question (page 4) that asks if your agency collects personal information. If your agency does not collect personal information, the survey will direct you to the final page to submit your response.

Some questions in the survey use branching logic to ask additional questions based on your responses. In this document, answers have been pre-selected to show all possible questions you may be asked.

Thank you for your attention to this important assessment! Please send any questions to [privacy@watech.wa.gov](mailto:privacy@watech.wa.gov).

## Privacy Assessment Survey Sections

Introduction

Agency Information

Personal Information

1. Types of Personal Information

2. Privacy Roles & Staffing

3. Training and Policies

4. Transparency

5. Individual Participation

6. Accountability

7. Data sharing, third party management and data publishing

8. Data inventory, retention and destruction

9. Future Planning

Conclusion

*RCW [43.105.369](#)*

*Office of Privacy and Data protection.*

(1) The office of privacy and data protection is created...

(3) The primary duties of the office of privacy and data privacy are:

(a) To conduct an annual privacy review.

## Survey Introduction and Disclosure Cover Page

# Introduction and Disclosure

### Welcome to the 2022 Privacy Assessment Survey

[RCW 43.105.369](#) requires the Office of Privacy and Data Protection to conduct an annual privacy review of agency practices. Your responses will help us measure privacy maturity across state agencies and develop resources and trainings where they are most needed. The goal is to establish a common understanding of current practices, not to measure compliance with specific laws or a specific set of standards. We understand that agency functions and privacy requirements vary. What is a best practice for one agency may not apply to another.

If your agency does not control any personal information about Washington residents, please complete the *Agency Information* section and indicate you do not control personal information. The rest of the assessment does not need to be completed. "Personal information" is information about a natural person that is identifiable to that specific individual.

You may use the Next and Previous buttons to skip through the form to fill out questions in any order.

Thank you for your time. Please feel free to send any questions to [privacy@watech.wa.gov](mailto:privacy@watech.wa.gov).

**Metadata Collection Disclosure Notice:** The tool used for the collection of survey data automatically collects Internet Protocol (IP) addresses and latitude and longitude data (location data) of your internet service provider's nearest "point-of-presence" or PoP location. Precise location data is only collected if you use a static IP address.

[Save and Resume Later](#)

Progress

Next »

The tool used for the collection of survey data collects IP addresses and latitude and longitude data of your internet service provider for dynamic IP addresses or precise location data if you use a static IP address. Most people use dynamic IP addresses. This metadata disclosure is new to the 2022 survey.

## Agency Information

### Agency Information

**Agency Name\***

For your Agency Code see the [OFM website](#)

**Agency Code\***

**Person Submitting\***

First Name

Last Name

**Your email address\***

A copy of your form submission will to be sent to this address.

[Save and Resume Later](#)

« Previous

Progress

Next »

"Personal information" is information about a natural person that is identifiable to that specific individual.

Information can include, but is not limited to, data, text, voice, and video.

**Does your agency maintain personal information about Washington residents?\***

- Yes.
- No. My agency does not maintain any personal information about Washington residents.

[Save and Resume Later](#)

« Previous

Progress

Next »

If your agency answers no on this page – your agency does not maintain personal information, you will be taken to the conclusion of the survey when clicking the “Next” button.

## Survey Questions

### 1. Types of Personal Information

## 1. Types of Personal Information

### 1.1 What type of information does your agency maintain about Washington residents? (Check all that apply)\*

- Contact information
- Financial, billing, or account information
- Social security numbers
- Driver's license numbers
- Other unique identifiers
- Date of birth
- Demographic information (e.g., race, ethnicity)
- Medical information
- Employment information
- Education information
- Justice information (e.g., criminal record)
- Familial information (e.g., household size, number of children)
- Immigration or citizenship information (e.g., place of birth, national origin, legal status)
- Specific geolocation information
- Biometrics
- Facial recognition templates
- Other:

### 1.2 How does your agency collect information? (Check all that apply)\*

- From people directly
- From other WA state agencies
- From federal agencies
- From local governments or other states
- Data brokers or similar entities
- From organizations we regulate or license
- From service providers (e.g., health care provider)
- Automated systems, such as cameras or GPS
- Other:

**1.3 Does your agency maintain any biometric identifiers?\***

- We do not collect, capture, purchase or obtain any biometric identifiers
- We likely have historical biometric data but do not currently collect biometric identifiers
- We do not have biometric identifiers but plan to collect them in the future
- We do collect biometric identifiers

**1.4 Does your agency use privacy impact assessments, risk registers, or other tools to assess privacy risks when beginning new projects that involve personal information?\***

- Yes  No

[Save and Resume Later](#)

« Previous

Progress

Next »

If you answer “yes” to question 1.4, you will be asked to explain further:

**1.4 Does your agency use privacy impact assessments, risk registers, or other tools to assess privacy risks when beginning new projects that involve personal information?\***

- Yes  No

**If yes, explain\***

[Save and Resume Later](#)

« Previous

Progress

Next »

## 2. Privacy Roles and Staffing

### 2. Privacy Roles & Staffing

**2.1 Choose the option that best describes who works on privacy in your agency:\***

- We have a person designated to set policy and handle questions for our agency, whose primary function is privacy and related issues
- We have a person designated to set policy and handle questions for our agency, but privacy is not their primary function
- We have a group of people who tend to work on privacy issues, according to their expertise
- We do not have a dedicated person or group, but tend to give these questions to internal staff such as the CIO or risk manager as appropriate
- We do not have internal staff with expertise, but we call outside experts when necessary

**2.2 Do you have a person designated to set policy and handle privacy questions?\***

- Yes
- No

[Save and Resume Later](#)

« Previous

Progress

Next »

Question 2.2 will ask for details concerning your designated privacy person if “yes” is selected:

**2.2 Do you have a person designated to set policy and handle privacy questions?\***

Yes  
 No

**Name\***

<input type="text"/>	<input type="text"/>
First Name	Last Name

**Email of designee\***

**Title\***

**Place in organizational structure \***

e.g., legal, risk management, information governance, IT

**What other positions work on privacy issues in your agency?**

[Save and Resume Later](#)

If “no” is selected, there is also more information required.

**2.2 Do you have a person designated to set policy and handle privacy questions?\***

- Yes
- No

**What positions work on privacy issues in your agency?\***

### 3. Trainings and Policies

## 3. Training and Policies

**3.1 Does your agency have formal policies and procedures that address privacy?\***

- Yes
- No
- Other:

**3.2 Does your agency have formal policies or procedures, or other standards, that address heightened protections for particularly sensitive subsets of information?\***

- Yes, we have formal policies or procedures that address heightened protections for particularly sensitive information
- We have standards that address protections for particularly sensitive information, but they do not rise to the level of formal policies or procedures
- We maintain some subsets of particularly sensitive information but do not have policies, policies, or standards that address heightened protections
- We do not maintain this type of information

**3.3 Does your agency offer employees privacy training? (Check all that apply)\***

- Agency-specific privacy training is available to staff
- Generic privacy training is available to staff
- Training is mandatory for all staff
- Training is mandatory for certain staff
- We do not offer privacy training
- Other:

**3.4 The state Office of Privacy and Data Protection has recently launched a general privacy training in The Learning Center called "Privacy Basics for Washington State Employees." The training takes approximately 40 minutes to take. Were you aware of this training?\***

- Yes
- No

**3.5 Will you consider making the "Privacy Basics for Washington State Employees" training mandatory:\***

- Yes, for all employees
- Yes, but only for employees who handle personal or confidential information
- Maybe, we need to learn more about the training
- No, we already have mandatory training
- No, not at this time
- No, our agency does not have access to The Learning Center

**3.6 The Washington State Agency Privacy Principles are a set of fundamental principles that help guide agency practices and establish public trust. Does your agency have policies that address these principles? (Check all that apply)\***

- Lawful, fair and responsible use
- Data minimization
- Purpose limitation
- Transparency & accountability
- Due diligence
- Individual participation
- Security

Link to the [Washington State Agency Privacy Principles](#)

[Save and Resume Later](#)

« Previous

Progress

Next »

Questions 3.4 and 3.5 are new to the 2022 survey. *Privacy Basics for Washington State Employees* is a new online training offered by the Office of Privacy and Data Protection.

## 4. Transparency

### 4. Transparency

**4.1 Do you have a website privacy policy that addresses information you track or gather on your website?\***

- Yes
- We have a website, but we do not have a website privacy policy
- We do not have a website

**4.2 Does your agency have an external-facing privacy notice or policy that explains how you collect, use, and disclose personal information?\***

- Yes
- No

This type of notice is separate from a website privacy policy that addresses information you track or gather on your website.

[Save and Resume Later](#)

« Previous

Progress

Next »

If “yes” is selected in 4.1, more information is required:

**4.1 Do you have a website privacy policy that addresses information you track or gather on your website?\***

- Yes
- We have a website, but we do not have a website privacy policy
- We do not have a website

**4.1.1 How current is your website privacy policy?\***

- Updated or reviewed in the past year
- Updated or reviewed in the last 5 years
- More than 5 years since last update or review

If “yes” is selected for question 4.2, two more questions are asked:

**4.2 Does your agency have an external-facing privacy notice or policy that explains how you collect, use, and disclose personal information?\***

- Yes
- No

This type of notice is separate from a website privacy policy that addresses information you track or gather on your website.

**4.2.1 How is your privacy notice or policy provided to people? (Check all that apply)\***

- In-person
- Mail
- E-mail
- Posted on agency website
- Other:

**4.2.2 What does your privacy notice or policy include? (Check all that apply)\***

- 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 for more information

## 5. Individual Participation

### 5. Individual Participation

**5.1 Does your agency have policies and/or procedures that address a person's request to control their personal information?\***

Yes  No

[Save and Resume Later](#)

If "yes" is selected for question 5.2 a follow up question is required:

### 5. Individual Participation

**5.1 Does your agency have policies and/or procedures that address a person's request to control their personal information?\***

Yes  No

**5.1.1 Which types of requests do the policies and/or procedures address? (Check all that apply)\***

- Requests to access or receive information
- Requests to correct information
- Requests to delete information
- Requests for information to be shared or sent to another person
- Requests for a restriction in how information is used or shared
- Other:

[Save and Resume Later](#)

## 6. Accountability

### 6. Accountability

**6.1 Has your agency experienced any data incidents in the past year? An incident occurs when there is an unauthorized use or disclosure, regardless of whether it rises to the level of requiring notification. (Check all that apply)\***

- We are not aware of any data incidents in the past year
- We experienced one or more data incidents which did not rise to the level of a breach that required notification
- We experienced one or more data incidents which required breach notification

**6.2 In the past year, have third parties your agency shares data with experienced any data incidents that involved agency data? (Check all that apply)\***

- We are not aware of any data incidents in the past year
- Third parties experienced one or more data incidents that involved agency data but did not rise to the level of a breach that required notification
- Third parties experienced one or more data incidents involving agency data that required breach notification

**6.3 What controls does your agency have in place to identify and respond to data incidents? (Check all that apply)\***

- A designated person or persons to make breach determinations
- Specific data breach procedures that identify roles and responsibilities
- Data breach procedures that identify roles and responsibilities, within a more general incident response plan
- Agency policies that require staff to report potential breaches
- Staff are trained on incident reporting responsibilities
- Data breach assessment templates or tools to document and guide breach determinations
- System monitoring or automated alerts
- Insurance that covers data breach response, such as notifications, credit monitoring, and legal counsel
- Other:

**6.4 Is your agency subject to data breach notification requirements other than RCW 42.56.590?\***

Yes  No

See [RCW 42.56.590](#) (Washington's data breach notification law)

**6.5 What type of security protections does your agency have in place to protect the privacy of personal information? (Check all that apply)\***

- Physical safeguards (e.g., key card access)
- Technical safeguards (e.g., encryption)
- Administrative safeguards (e.g., policies and procedures)
- Other:

**6.6 Does your agency collect any metrics about your privacy program?\***

Yes  
 No

[Save and Resume Later](#)

« Previous

Progress

Next »

Question 6.4 asks for more information if “yes” is selected:

**6.4 Is your agency subject to data breach notification requirements other than RCW 42.56.590?\***

Yes  No

See [RCW 42.56.590](#) (Washington's data breach notification law)

**Please list or briefly describe other data breach notification requirements you must comply with (e.g. HIPAA, SSA, GLBA, etc.)\***

Question 6.6 is new this year. If your agency does keep metrics, this question expands for more details:

**6.6 Does your agency collect any metrics about your privacy program?\***

- Yes
- No

**Which topics do the metrics cover? (check all that apply)\***

- Audits
- Complaints
- Data retention or destruction
- Data sharing agreements
- Incidents/breaches
- Maturity model progress or privacy framework adoption
- Privacy impact assessments
- Requests for personal information
- Other individual participation (to modify, delete, etc.)
- Training
- Other:

## 7. Data Sharing, Third Party Management, and Data Publishing

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

**7.1 Who does your agency share personal information with? (Check all that apply)\***

- Other state and local agencies
- Federal agencies
- Law enforcement (as part of our data sharing relationship)
- Law enforcement (on ad hoc basis, as required)
- Researchers
- Vendors working on agency's behalf
- Data brokers
- Service providers (e.g., health care provider)
- Other:

**7.2 Does your agency sell personal information?\***

- Yes    No    Not sure

**7.3 How are requests to establish new data sharing relationships vetted? (Check all that apply)\***

- Individuals make decisions based on program needs
- Individuals make decisions pursuant to established policies
- Only designated individuals can approve data sharing
- There is a review process to ensure contracting, privacy, and security are considered before establishing new data sharing relationship
- The agency has a formal committee to approve data sharing requests
- Other:

**7.4 Which elements are part of your agency's data sharing agreements? (Check all that apply)\***

- Confidentiality terms and conditions
- Notice of data breaches
- Notice of data incidents, regardless of whether they are a breach that requires notification
- Data security requirements
- Attestation of appropriate privacy and security practices
- Data security audits
- Data use audits
- Permissible uses
- Data breach insurance coverage
- Nondisclosure or confidentiality agreements
- Training for people who will have access to data
- Other:

**7.5 What steps has your agency taken to comply with ESSB 5432, sections 5 and 6?\***

- Modified existing Data Sharing Agreement (DSA) language
- Reviewed contracts for DSA language
- Entered new DSAs to document existing data sharing relationships
- Implemented new policies, processes, or other controls to ensure appropriate DSAs are executed
- Other:

Link to ESSB [5432](#)

**7.6 What barriers or challenges does your agency face in complying with ESSB 5432, sections 5 and 6?**

(Optional)

**7.7 Does your agency have standards or processes to minimize the risk of re-identification when information is publicly disclosed? (Check all that apply)\***

- No
- De-identification standards
- Small numbers standard
- Privacy review of published data
- Other:

[Save and Resume Later](#)

« Previous

Progress

Next »

## 8. Data Inventory, Retention, and Destruction

### 8. Data inventory, retention, and destruction

**8.1 Has your agency completed data mapping or an inventory of agency systems and applications, including the types of personal information included?\***

- Yes
- No
- We are in the process of completing one
- Other:

**8.2 Has your agency completed data mapping or an inventory that includes data or information stored outside of systems and applications?\***

- Yes
- No
- We are in the process of completing one
- Other:

**8.3 When was your last records inventory?\***

- Within the past year
- Within the past 2 years
- Within the past 5 years
- Unsure
- Other:

See [RCW 40.14.040](#)

**8.4 How does your agency delete data? (Check all that apply)\***

- Our records officer is responsible for deleting old data
- Programs or work units are responsible for deleting data according to retention schedules
- We use automated tools to delete old data
- We rarely delete old data

Save and Resume Later

« Previous

Progress

Next »

## 9. Future Planning

### 9. Future Planning

#### 9.1 How important is privacy for your agency this year?\*

Rate this on a scale of 1-10 with 10 being essential to the agency strategic plan, and 1 being not relevant for the coming year

#### 9.2 Over the last two years, has the importance of strong privacy protections for your agency:\*

- Increased
- Decreased
- Stayed about the same

#### 9.3 What privacy tasks is your agency planning to work on in the next year? (Check all that apply)\*

- Review and/or update privacy policies
- Update or create privacy training
- Review and/or update privacy notices
- Review and/or update data sharing agreements
- Create or update data map or inventory
- Implement or update privacy impact assessment process
- Other:

#### 9.4 What developments or projects most improved your agency's privacy posture in the past year?

**9.5 Have you or employees from your agency attended or watched an Office of Privacy and Data Protection webinar in the last year?\***

- Yes
- No
- Unsure

Link to webinars: <https://watech.wa.gov/privacy/gov-agency-resources>

**9.6 Do you have suggested topics you would like to see covered in OPDP webinars in the next year?**

 1000/1000

**9.7 To your knowledge, has your agency reviewed or used any of the following resources to improve its privacy and data governance practices?**

- Data Breach Assessment Form
- Data Request Template
- Data Share Template(s)
- Data Share Implementation Guidance
- Privacy by Design
- Other:

(check all that apply)

See additional resources for the question to the left:

<https://watech.wa.gov/privacy/gov-agency-resources>

**9.8 What other specific resources or training topics would be helpful to your agency?**

(Optional)

**9.9 What was your level of satisfaction in your interactions with OPDP over the past year?**

**9.10 Please share any other thoughts or suggestions based on your interactions with the OPDP**

[Save and Resume Later](#)

« Previous

Progress

Next »

Question 9 is changed slightly from the 2021 survey. OPDP greatly appreciates your feedback in this question.

## Conclusion

### Conclusion

This is the end of the privacy assessment form. Feel free to click the **Previous** button to review your answers.

When you click the SUBMIT button, you will be shown questions you forgot to answer.

A copy of this form submission will be sent to your email address

If you have any questions or comments, please contact [privacy@watech.wa.gov](mailto:privacy@watech.wa.gov). We also appreciate a review of the form below.

**Your comments about this form:**

(Optional)

I am ready to submit this form

[Save and Resume Later](#)

[« Previous](#)      [Progress](#)      [Submit Form](#)

Upon submission, the form logic will check to make sure all fields with a red asterisk (\*) are completed. If any required questions are not completed, you will be returned to that field of questions. A completed copy in .pdf format will be sent to the email address you provide. Questions or comments about the survey can be directed to [privacy@watech.wa.gov](mailto:privacy@watech.wa.gov).

Thank you for your attention to this important assessment for the state.