



Privacy Notice Implementation Guidance

July 2024 | Office of Privacy and Data Protection

Table of Contents

Background	3
How to use this guidance	3
Implementation Considerations	4
Definitions	4
Distinguishing from other document types	4
Plain language	5
Accuracy and currency	5
Method of delivery	5
Timing	6
Formatting	7
Privacy Notice Content	8
The types of personal information the agency processes	8
How and why the agency processes personal information	9
Who the agency shares information with, if applicable	9
How individuals can exercise any applicable rights to access or control their information ..	10
How to contact the agency	10
Other resources	11
Contact.....	11

Background

Privacy notices are external facing documents that explain how an agency collects, uses, shares, manages and protects personal information. They also include how individuals can control their information and who to contact for more information.

Privacy notices are specifically required by the General Data Protection Regulation in the European Union, the California Consumer Privacy Act, and many other state and federal laws. For Washington state agencies, privacy notices are required by [Executive Order 16-01](#), Sec. 5 and the [Washington state Privacy and Data Protection Policy](#), Sec. 10. They also support NIST 8–53, Rev. 5, PT-5, and the Communicate function of the [Washington Privacy Framework for State Agencies](#). Some agencies have additional privacy notice requirements under laws like the Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), or Children’s Online Privacy Protection Act (COPPA).

Providing transparency about agency practices is an important piece of effective privacy protection, but notices alone cannot address all privacy risks. Privacy notices should be implemented as part of a broader approach to privacy that includes implementing all of the [Washington State Agency Privacy Principles](#).

How to use this guidance

The types of personal information, how that information is collected, used and shared, and the laws that processing is subject to varies significantly across different state agencies. Privacy notices that describe those practices necessarily vary as well.

This guidance is broken into two main parts:

- The Implementation Considerations section includes general considerations to keep in mind while crafting or revising a privacy notice. It also includes information about some of the choices to make about implementation, such as format, timing and method of delivery.
- The Privacy Notice Content section includes additional explanation about each element required by the Washington state Privacy and Data Protection Policy.

This document should be used as a starting place when undertaking a new privacy notice, or to help review existing privacy notices to ensure all key elements are included. It only provides a general overview that is broadly applicable to different types of agencies. Specific agency functions will require different language. Some agencies are subject to laws that include additional transparency requirements. Those laws may dictate timing, method of delivery, or additional elements that need to be included.

Nothing in this document is or is intended to be legal advice. Agencies should consult with legal counsel for legal questions that come up while writing or implementing privacy notices.

Implementation Considerations

Aside from creating the documents themselves, there are several important considerations to keep in mind for privacy notice implementation. These include:

- Understanding how privacy notices fit in with other privacy documentation,
- Making the notices accessible for the target audience,
- Keeping notices current, and
- Determining how, when and in what format notices will be delivered.

Definitions

Aggregate data - Information about groups or categories of individuals that does not, and cannot reasonably be used to, identify specific individuals.

Anonymous data - Information that does not directly or indirectly, and cannot reasonably be used to, identify a specific individual.

Personal information - Information that is identifiable, directly or indirectly, to a specific individual.

Process - Operation or set of operations performed upon personal information that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer and disposal of personal information.

Distinguishing from other document types

Although sometimes used interchangeably, privacy notices are distinct from privacy policies (which are internal documents). They are also normally distinct from website privacy notices (which typically cover only the information that is automatically collected when a person browses a website).

	Privacy Notice	Website Privacy Notice	Privacy Policy
Aliases	Privacy Statement, Privacy Policy, Notice of Privacy Practices	Cookie Notice, Security Notice, Privacy Notice, Privacy Statement, Privacy Policy	
Associated principle	Transparency	Transparency	Accountability
Audience	External	External	Internal

Plain language

Privacy notices are intended to be read by external customers, who are often unfamiliar with privacy and data processing terms and concepts. Agencies should avoid legalese and make notices as concise and approachable as possible. Where it is impossible to remove terms of art without reducing accuracy, those terms should be clearly explained.

The people reading privacy notices may not use English as a primary language. Privacy notices should typically be translated to and available to a person in the language your agency normally interacts with them in. Your agency may have more specific guidance on when and how to translate documents.

Accuracy and currency

Privacy notices are only meaningful if they contain accurate information about agency practices. Gathering accurate information requires working across disciplines to understand the intended purposes for processing personal information, the commitments for how that information will be processed, and verifying the actual practices in place. For example, legal services may be able to define legal requirements but business teams need to be involved to confirm what they have implemented. Communication teams may have the best information about how information is automatically collected on websites, data teams may have the best insight into data sharing activities, information technology teams may know the most about role-based access, and so on. Except in very small agencies or agencies that process very little personal information, privacy notices can rarely be written by a single person.

To stay accurate, privacy notices also need to stay current. Legal requirements can change over time. Processing activities change as agencies launch new programs or improve existing ones. And technology changes frequently on purpose as systems are updated, and incidentally as software features and vendor practices change. All these types of changes justify frequently reviewing privacy notices. WaTech recommends reviewing at least annually, or anytime there are material changes to practices.

Method of delivery

There are many options for how to deliver or otherwise make privacy notices available. Those options include at least:

- Linked on website footer
- Linked as part of web form when people submit personal information
- E-mailed
- Handed to someone in person
- Posted in physical location for viewing
- Mailed to physical address

- Just-in-time electronic notice at point of information collection

The right choice or choices will depend on how your agency typically interacts with the people it is collecting information from. For example, if your agency does not interact with people in person or collect physical addresses, then there is no option to provide a physical copy. Similarly, if your agency collects information through intermediaries and rarely has a direct relationship with people, posting online may be the only feasible option. But if your agency has offices that people routinely visit, posting a physical copy could be the best option to ensure people have an opportunity to review.

Consider whether to gather acknowledgement that a privacy notice was received. A signature could be used to confirm a physical copy was delivered in person. If a customer is specifically opting in to voluntary processing (such as by providing optional information or authorizing specific sharing), then acknowledgment should be part of the consent process.

Some privacy laws have specific requirements for the way or ways that privacy notices must be delivered.

Timing

When privacy notices are provided should also be carefully considered. There are three primary options for when to provide privacy notices. In many cases all three should be used.

- Initial privacy notice. A privacy notice should be available during an initial interaction with a person. This may occur by being posted or delivered in a physical setting, being linked on a website, or provided electronically when a person signs up for a service.
- Periodic privacy notice. When an agency regularly has ongoing relationships with people, it may be appropriate to provide routine periodic updates. These serve as reminders of both the fact that the agency is processing personal information, and the specific ways the agency is processing that information.
- Revised privacy notice. Updated privacy notices should be provided when there are material changes to privacy practices or the way the agency is processing personal information. Updated privacy notices should not be retroactive – they should be provided prior to material changes going into effect.

Some privacy laws have specific requirements for when privacy notices must be delivered. For example, a health plan subject to HIPAA must provide an initial notice at the time of enrollment for new enrollees, at least every three years after that, and when there are material changes. Financial institutions subject to GLBA must provide an initial notice, an annual notice, and a notice when there are material changes.

Formatting

Transparency is most effective when information is provided in a variety of formats. In addition to a complete privacy notice, other formats can help explain information in an understandable way. Those include:

- Layered privacy notices. These notices include short explanations of the most important information, and additional layers with more details.
- Dashboards. Privacy dashboards are interactive tools that tell people how you use their information and allow them to manage their preferences about how you process it.
- Just-in-time notices. Just-in-time notices are provided right before a person provides personal information or consents to a particular type of processing. Examples include a link to a privacy notice right before a person submits a web form, or a pop-up explaining why a specific data element is needed as a person completes a form.

Privacy Notice Content

The Washington state Privacy and Data Protection Policy, Data-03, requires privacy notices to include:

- The types of personal information the agency processes
- How and why the agency processes personal information
- Who the agency shares personal information with, if applicable
- How individuals can exercise any applicable rights to access or control their personal information
- How to contact the agency

These categories are broadly applicable to different types of agencies and personal information processing. Some agencies are subject to more specific privacy notice requirements that may have additional or more specific privacy notice requirements.

The types of personal information the agency processes

Privacy notices should inform people of the types or categories of personal information your agency processes. This information should be detailed enough to be meaningful, but it does not need to include specific data elements.

The appropriate level of detail will vary depending on the types, volume and variety of personal information it collects. The level of detail may also vary depending on whether it is provided directly from people. When information is provided directly, such as by filling out forms or submitting surveys, people have a better understanding and control of what is being provided. Privacy notices should be more explicit when agencies collect information that people are less likely to be aware of. This includes automated online tracking using technologies like cookies, pixels or web beacons. It also includes information collected from third parties, like service providers or data brokers.

Examples of categories of personal information include demographic information, biometric information, communications, location information and website usage. In addition to describing how personal information is processed, privacy notices should also explain what anonymous or aggregate information is used, if applicable.

How and why the agency processes personal information

This is a broad category that includes most types of processing. The chart below covers important topics to include. They are broken up to emphasize things to consider, but when actually writing a privacy notice there will likely be significant overlap.

Topic	Explanation
Overall purpose	Introduce your agency. Explain its overall purpose and the functions it performs or services or benefits it provides.
Type of data	Describe what kind of personal information is collected as described above.
Specific uses	Explain how your agency uses the personal information it collects. This makes a connection between what information is collected, and why that information is collected. In most cases there are different uses for different types of information. For example, different types of information may be collected to provide services, verify identity and detect fraud, and improve website performance.
Methods of collection	Explain not just what information is collected, but how it is collected. This should include the ways your agency interacts directly with individuals, such as with web forms or over the phone. It should also include the ways personal information is collected automatically or from third parties.
Who data is shared with	Describe types of third parties information is shared with. If your agency sells personal information, that should be specifically addressed. See below for more details.
Retention and deletion	Describe applicable retention and deletion commitments. This may be a general statement about only retaining information as long as needed for the original purpose or as otherwise required by law.
Data security	Explain your agency's commitment to protecting data and general statement of security practices.

Who the agency shares information with, if applicable

Privacy notices should separate how an agency shares information from how it uses information. The description should include at least:

- Who information is shared with. Describe the types of third parties information is shared with. If your agency sells personal information, that should be specifically addressed.
- Why it is shared. For each category of recipient, describe the purpose of sharing the information. For example, information may be shared with a vendor to perform functions on behalf of the agency, with a service provider to enable them to provide services directly to people, to researchers for appropriately approved human subject research, or to data brokers to fulfill a legislative mandate.
- How it is protected once shared. Describe whether the information is still subject to the same level of protections once it is shared. For example, explain whether vendors have agreed to the same level of protections that are described in the privacy notice, or whether the information is instead subject to the privacy practices of the recipient.

How individuals can exercise any applicable rights to access or control their information

Agencies must allow people to access or control their information to the extent consistent with applicable law and the government functions the agency performs. Examples of individual participation include confirming whether an agency processes personal information, accessing or correcting information, asking for information to be deleted, opting in or out of particular uses or disclosures, and withdrawing prior consent. The types of individual participation allowed by your agency should be described, together with how to exercise that control.

At a minimum, privacy notices should explain how a person can access their own information. For many agencies individual access is done through public records request processes. For some agencies, this may also be possible through self-service portals.

How to contact the agency

Privacy notices need to clearly identify how to get additional information, ask questions or make complaints. At a minimum this should include contact information for the appropriate agency contacts.

Other resources

Privacy notices of private sector companies aren't typically directly applicable to Washington state agencies, because those companies process personal information for different purposes and subject to different laws. But here are some examples for inspiration:

- [The Walt Disney Company](#)
- [Google](#)
- [Airbnb](#)
- [Pinterest](#)

At the state level, the Washington Department of Licensing has a comprehensive [Privacy Center](#) that includes a clear overview of privacy practices, as well as real examples to help make the agency's data practices understandable. It has a layered approach that allows individuals to explore the areas they are most interested in.

Federal agencies have also issued model notices for organizations subject to HIPAA, FERPA, and GLBA:

- HIPAA Model Privacy Notice Template from U.S. Health and Human Services Office of Civil Rights: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html>
- FERPA Model Annual Notices from U.S. Department of Education: <https://studentprivacy.ed.gov/annual-notices>
- GLBA Model Privacy Form from U.S. Securities and Exchange Commission: https://www.sec.gov/rules/final/2009/34-61003_modelprivacyform.pdf

Contact

Need more information? Send questions to privacy@watech.wa.gov.