WaTech
Washington Technology Solutions

Sometimes Asked Questions

Office of Privacy and Data Protection

April 2024

WaTech
Washington Technology Solutions

- General questions
- Data sharing agreements
- Privacy assessments
- Data classification
- Artificial intelligence

* This presentation is for general informational purposes and is not legal advice. The information provided reflects the Office of Privacy and Data Protection's current understanding. Best practices change over time and according to context. You should consult your attorneys on specific legal questions.

Why do we need a privacy officer?

- Privacy has overlap with other disciplines
- It is also its own discipline that requires (1) specific expertise and (2) sufficient bandwidth to run privacy workstreams
- Privacy professionals help reduce risk, increase trust, and bridge gaps
  - E.g., Business may define system requirements, and the security team keeps it secure. Privacy helps define what is collected, how it can be used, and who can use it.

Why do we need a privacy officer?

- The scope of privacy work is only increasing
  - Legal requirements and new policy considerations are rapidly evolving
  - Privacy will continue to have an increased role in WaTech's oversight functions and should have an increased role within agencies, too
  - Privacy professionals support essential functions like incident response and data sharing agreement implementation
  - Privacy has a significant role in AI governance

Is x,y,z personal information?

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

Personal information – key concepts

- Not limited to Category 3 or 4 information
- Broader than definition in RCW 42.56.590
- Can include information without direct identifiers

WaTech
Washington Technology Solutions

Can data be sent or hosted outside the US?

- Currently no state policy restriction on "offshore" data hosting.*
- *However, several caveats:
  - Applicable federal laws
    - IRS 1075
    - CJIS data restrictions
- Executive Order 14117 - Restrictions and prohibitions on sharing American personal data with "countries of concern"
- International travel technology policy restrictions & requirements

WaTech
Washington Technology Solutions

Can data be sent or hosted outside the US?

Other Considerations:

- Lack of legal protections
- Lack of recourse
- Consider including offshore prohibitions in procurements

If data is going to be transferred, it's best to at least:

- Ensure an appropriate documentation and acceptance process to understand and sign-off on non-US locations
- Consider the criticality and sensitivity of the information, including the impact caused by the loss of confidentiality, integrity or availability
- Consider that some jurisdictions are safer than others. E.g., GDPR provides significant protections for data in EU member states, but data stored in China is subject to government surveillance

WaTech
Washington Technology Solutions

Can we use ad tracking pixels?

- Inserting pixels for ad tracking purposes is not prohibited by law for government agencies in WA.
- Best Practices for Privacy
  - Transparency
  - Opt-out choices
  - Update Privacy Policy
  - HIPAA requirements

Determine the following and then add the information to your website:

- What personal data are you collecting?
- Where are you collecting it from?
- Where will it be stored?
- Who will have access?
- Purpose for collection? (Why do you need it?)
- How long does it need to be retained?

WaTech
Washington Technology Solutions

Data sharing agreements

Which RCWs require Data Sharing Agreements?

External Contractors

- RCW 39.26.340(1) states that "[b]efore an agency shares with a contractor category 3 or higher data, as defined in policy established in accordance with RCW 43.105.054, a written data-sharing agreement must be place." Within chapter 39.26 RCW, agency means office or activity of the executive or judicial branches of state government.

Other public entities

- RCW 39.34.240(1) states that "[i]f a public agency is requesting from another public agency category 3 or higher data . . . the requesting agency shall provide for a written agreement between the agencies . . . ." Within chapter 39.34 RCW, a public agency means any agency, political subdivision, or unit of local government; any state agency; any United States agency; any federally recognized tribe; and any political subdivision of another state.

WaTech
Washington Technology Solutions

Which policies do RCW 39.26.340 and 39.34.240 refer to?

- …policy established in accordance with RCW 43.105.054
- This RCW is WaTech's authorizing statute that provides authority to develop state IT standards and policies.

- Data Classification Standard
- Data Sharing Policy

What is a DSA? Can terms of service satisfy DSA requirements?

- DSA = Data Sharing Agreement
- Defined in policy not law
- Substance over Form – this means a DSA is not required to be its own stand-alone agreement as long as terms meet DSA policy requirements
- Terms of Service can satisfy DSA requirement if the terms meet DSA policy requirements
- E.g. the terms include data handling and protection requirements requisite to the risk of data
- If high risk use case though TOS may not be sufficient

What is difference between DSA/NDA

- DSA is the Agreement you have with the third party with all of the required terms and conditions regarding data handling and protection.
- DSA's may require third party employees to sign NDAs to handle confidential information

- NDA = Non-disclosure Agreement
- NDAs or non-disclosure agreements, are legally enforceable contracts that create an obligation between a person or entity who has sensitive information and the person who will gain access to that information.
- It requires the person with access to keep the information confidential.

What if vendor refuses to have employees sign nondisclosure agreement (NDA)?

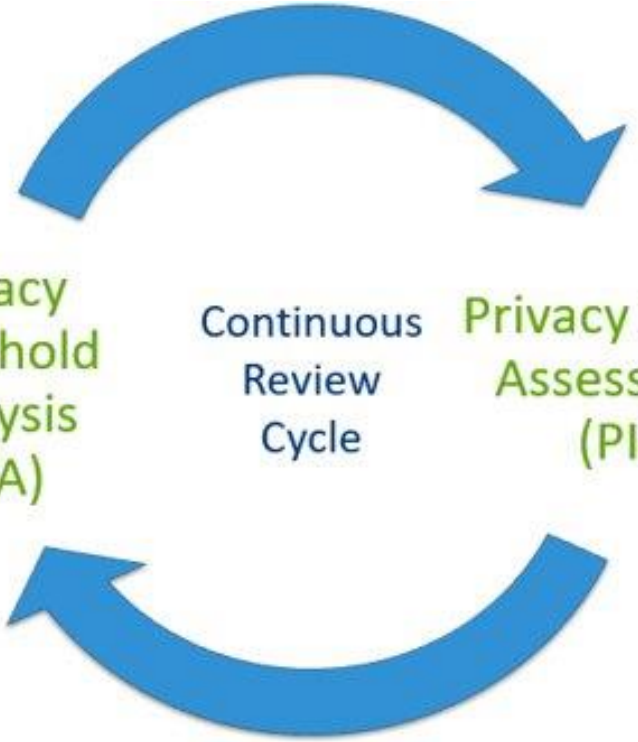
- Data recipients limited to authorized use by authorized users
  - NDAs *one way* to obtain assurance
- Alternative – Vendor must ensure that users will sign agency NDA or have a substantially equivalent agreement or obligation
- E.g., Sample DSA #2, page 5

WaTech
Washington Technology Solutions

Privacy assessments

What is the difference between a PTA and PIA?

A PTA is a brief, high-level assessment used to determine whether the subject of the review may have privacy implications and require a PIA.



The PIA is a tool designed to help consider how privacy principles have been incorporated into the project, assess privacy risks and how they should be appropriately mitigated, and document these findings.

When is a PIA required?

Factors that could indicate heightened risk	
Considerations for sensitive information	Considerations for processing activities
Race or ethnicity	Selling data
Religious or philosophical beliefs	Using new technologies
Mental or physical health	Monitoring geolocation
Sex life or sexual orientation	Large scale processing, including monitoring a public place on a large scale
Citizenship or immigration status	Using data to make automated decisions that could have legal or similarly significant effects
Genetic or biometric information	Profiling that could foreseeably lead to unfair or disparate impact on individuals
Information about minors	

Who should complete the PTA?

- PTA is a brief assessment that considers:
  - Type and amount of information
  - Business purpose and uses
  - Technology implementation
- Appropriate person varies between agencies
  - Might be multidisciplinary
- Make sure the PTA includes BOTH business purpose and technology overview

WaTech
Washington Technology Solutions

What if we don't have complete information when completing the PTA?

Describe best available information, including known and unknown information		
New program with unknown scope -> Estimate based on planned scope, experience with similar programs	Determinations have not been made or processes not in place -> Describe aspects that are still to be determined, including existing commitments or plans for decision making process	Scope is likely to change -> Describe current scope; acknowledge potential changes including nature and timeline for changes

Who should complete the PIA?

- Unlike PTA, needs to be completed by multidisciplinary team
- Consider: Privacy, IT, cybersecurity, business team, legal, records management, information governance, risk, vendor

What is OPDP's role in approving PIAs?

- OPDP is available to:
  - Orient PIA participants to PIA process and expectations
  - Provide general guidance and answer specific questions that come up through the process
  - Review and comment on drafts, if requested
- Risk treatment decisions are ultimately agency decisions

Should my agency adopt internal PTA/PIAs processes and procedures?

- Yes
  - Document what is appropriate for your agency
  - Establish commitments before a project requires review

WaTech
Washington Technology Solutions

Data classification

WaTech
Washington Technology Solutions

Is x,y,z category 3?

Subject to public disclosure

Not subject to public disclosure

Category 1 – Public Information

. . . information that can be or currently is released to the public.
It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

Category 2 – Sensitive Information

. . . may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Category 3 – Confidential Information

. . . information that is specifically protected from either release or disclosure by law . . .

Category 4 – Confidential Information Requiring Special Handling

. . . information that is specifically protected . . . and for which [there are especially strict requirements and serious consequences could come from improper disclosure]

Is employee demographic data exempt from public disclosure?

The following employment and licensing information is exempt from public inspection and copying under this chapter (42.56.250):

. . .

- (l) Voluntarily submitted information collected and maintained by a state agency or higher education institution that identifies an individual state employee's personal demographic details.
- "Personal demographic details" means race or ethnicity, sexual orientation as defined by *RCW **49.60.040**(27), immigration status, national origin, or status as a person with a disability.
- This exemption does not prevent the release of state employee demographic information in a deidentified or aggregate format.

Is other demographic data collected from the public exempt from public disclosure?

- Probably not.
- To reduce risk:
  - Data minimization – Avoid collecting information you don't need
  - Purpose limitation – Clearly define purposes for collection
  - Transparency – Explain disclosure requirements, provide meaningful opportunity for consent
- Proactively evaluate when legislature considering new programs or functions

Is software code Category 3?

The following information relating to security is exempt from disclosure. . .

(4) Information regarding the public and private infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase the risk to the confidentiality, integrity, or availability of security, information technology infrastructure, or assets

-RCW 42.56.420

WaTech
Washington Technology Solutions

Does using MFA open personal devices up to public records disclosure?

- Authenticator apps

- Text based

WaTech
Washington Technology Solutions

Artificial intelligence

Can we use biometrics to unlock devices?

RCW 40.26.020 – "Unless authorized by law, an agency may not collect, capture, purchase, or otherwise obtain a biometric identifier without first providing notice and obtaining the individual's consent. . . ."

Chapter 43.386 RCW – Extensive requirements for use of facial recognition

- RCW 43.386.010(3)(b) - "Facial recognition service" does not include: (i) The analysis of facial features to grant or deny access to an electronic device. . .

Can we use biometrics to unlock devices?

Is the agency obtaining a biometric identifier?

Is the agency using biometrics for a purpose other granting access to a device?

What happens if someone uses an AI notetaking tool during a public meeting?

AI notetaking tools

- Transcribe spoken words to text and can create summaries and notes
- May be used to supplement participation, or when unable to attend

Considerations

- Is there an expectation of privacy?
- Public meetings often recorded already
- Is the tool malicious or otherwise disruptive?

What happens if someone uses an AI notetaking tool during an internal meeting? Considerations

- Is it an internal application or external?
- Applicable agency policies
- Expectations about meeting (context and type)
- Technical controls for disabling note takers
- Records (storage and production)
- WA is two-party consent state
  - RCW 9.73.030

Can agencies implement generative AI solutions?

- Yes, if they support business purposes as, or more effectively, than other available tools. Consider applicable risks.

Less risk	More risk
Category 1	Category 2, 3 or 4 information
Recommendations or suggestions that don't impact safety or fundamental rights	Automated decisionmaking, especially decisions that impact safety or fundamental rights
Internal facing	External facing
Agency governance and workforce education	Implemented without oversight or workforce education
Appropriate agreements	Free version
Controlled data inputs, high data quality	Poor or unknown data quality

WaTech
Washington Technology Solutions

Questions?

privacy@watech.wa.gov

www.watech.wa.gov/privacy