

Washington State Agency Privacy Principles and Risk Management

Office of Privacy and Data Protection March 24, 2022



Overview



- Privacy principles background
- Development of Washington State Agency Privacy Principles
- Risk management benefits





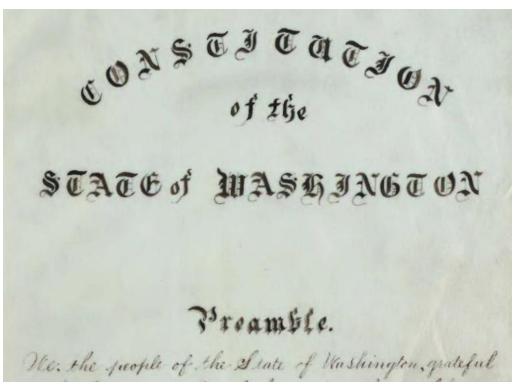


P D P



Washington's Consolidated Technology Services Agency

Privacy is important.







the universal declaration of **Human Rights**

resignation of the informat alignity and of the equal and elimitate eights of all members of the basson family is the functions. Josephin, justice and power in the world.

common acts which have another to the control of th

or the Aughted experience of the resources people,

containing it is executed, if more in sent to be competited to have recourse
or that rewest, to exhelicion against conserve and approxima, that havens

Amount is in second to pressure the disordepoint of friendly relations.

Being the peoples of the Casted Nations have in the Charter regions their fields in Jundemental Assesses rights, in the eligatey and worth a the houses present and in the rapid stable of man and recover and have determined to pressure social progress and faster simulately of $S_{\rm p}^{\rm to}$ in larger freedom.

Common Member Notes here pholyed themselves to unknow, in cospectation with the Existed Nations, the promotion of anisotral tragget for any observation of human rights and foundamental fundament

of the representation of the right and frequencies of the photon.

THE STREET, COMME

where the Fritzen Reduction of Human Rights in a communication of the decisional for all purpless and all attains, as the analytic activation of the decision of the control of the contro

and the first and the second section of

C Any Oraque, Mayon, principle of other spenses.

(§ 40 considering oraque, Marie of Marie oraque, Mari

Totale of scorages,

- The same first tenter or design or workers assessed and the first tenter or another and the first tenter.

The second is advantaged as the second as the second

promitted for the second secon

120

and the same of th

Response they the highest descriptions to public systems
 Response they the public shall be the latter of the contract
 Response they are the public to the latter of the contract
 Response the latter to the public to the latter of the contract
 Response the latter to the contract of the latter of the latte

med ments per a spiller in religion from the last members a species of a continue and a spirit religion to the first period for the spirit religion to the spirit period for the spirit of the secondary.

Selection of the select

prior tracing to filtrath and to facility of including models. Substituting the confidence of including to the beam point amortics.

The state of the last contract to the

The second has the option of an internal of thought party for the facility of and large, of the second and in facility and of the second and facility. The second and in facility and options of the second and internal or and address detailed. Which will be second at party for the second and the second and and an and facilities to the second and the second and facilities to the second and the second the second the second the second the s

desired desired in spire is proving to the control of acceptance and control of acceptance and control of acceptance and control of acceptance and acceptanc

And the second s

To the part of the State.

refused the of the contraction, to come the sent and to site obtained by the contraction and its boards.

If the contract to the contraction of th

AND ADDRESS OF THE PARTY OF THE

Department on the contraction of the contraction of

NITED NATIONS

What is Privacy?





Communications Privacy





Territorial Privacy





Bodily Privacy





Information Privacy



What is Privacy?





Communications Privacy



Territorial Privacy



Bodily Privacy



Information Privacy



P

D

P



Laws & Regulations

Privacy Principles

Privacy Frameworks

> Maturity Models

Effective Privacy and Data Protection

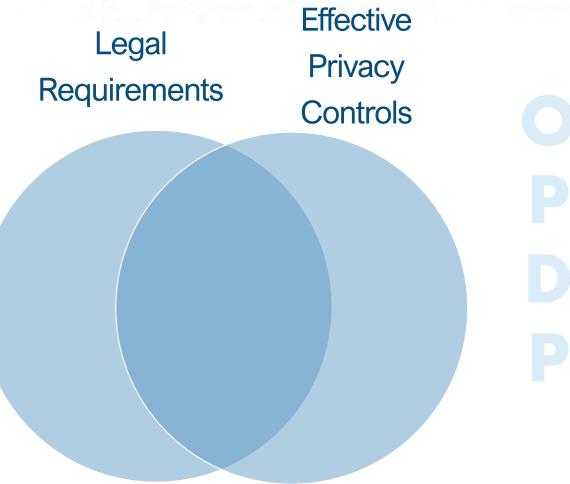
Laws and Regulations

Washington Technology Solutions

Washington's Consolidated Technology Services Age

Gaps may exist where laws:

- Do not establish strong enough protections to meet people's expectations
- Contemplate changes in technology and business practices
- Account for an organization's specific mission or cultural context







P D P

1973 Code of Fair Information Practices (FIPs)



- There must be no personal data recordkeeping systems whose very existence is secret.
- There must be a way for a person to find out what information about the person is in a record and how it is used.
- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the individual's consent.
- There must be a way for a person to correct or amend a record of identifiable information about the person.
- Any organization creating, maintain, using or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take precautions to prevent misuse of the data.

FIPPs Evolution



- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
- Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981)
- APEC Privacy Framework (2004)
- United Nations Personal Data Protection and Privacy Principles (2018)













OECD	APEC	UN
Openness	Notice	Transparency
Proportionality and Necessity	Collection Limitation	Collection Limitation Retention
Individual Participation	Choice Access and Correction	X

Inclusion in Privacy Laws



- Privacy Act of 1974
- General Data Protection Regulation (GDPR)
- Fair Credit Reporting Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Children's Online Privacy Protection Act (COPPA)
- California Consumer Protection Act (CCPA)









What's an agency to do?



- No complete consensus on principles
- No alignment between laws
- No wide applicability to all agencies



Primary OPDP Functions



"The primary duties of the office of privacy and data protection with respect to state agencies are:

. . . .

(c) To articulate privacy principles and best practices. . ."

RCW 43.105.369(3).

0

P

D

P

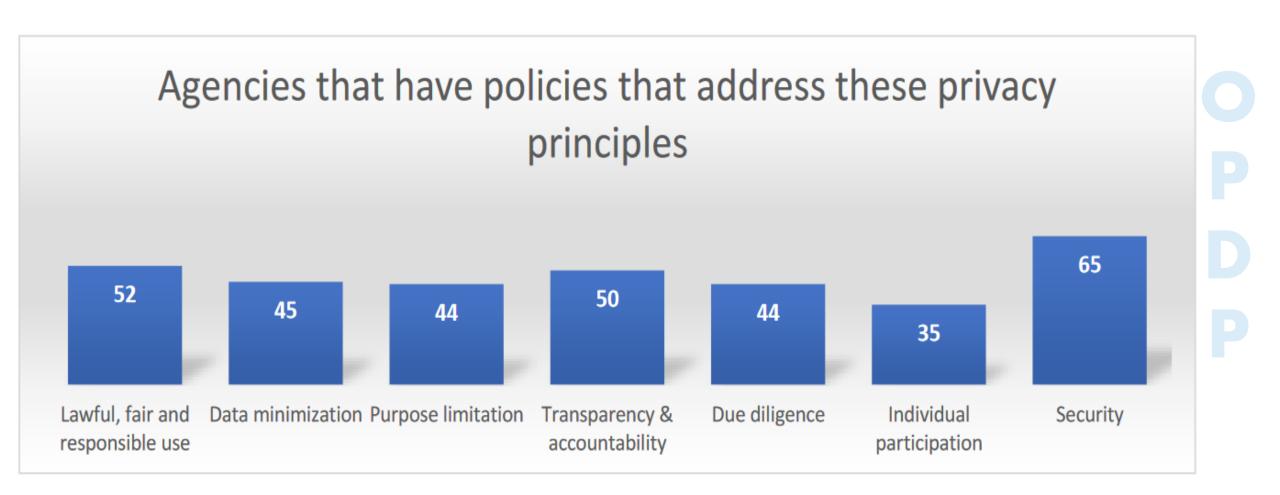


Washington's Consolidated Technology Services Agen

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









Principles and Risk Management

P D P



AND RESPONSIBLE USE

Collection and use is:

- Based on legal authority;
- Not deceptive;
- Not discriminatory or harmful; and
- Relevant and reasonably necessary for legitimate purposes



LAWFUL, FAIR, AND RESPONSIBLE USE



Implementation

- Only collect and use information with appropriate legal authority.
- Collect and use information fairly, meaning at a minimum that processing is not deceptive or unduly harmful.
- Collect and use information responsibly and ethically. This includes taking steps to ensure information gathered is accurate and correcting information that is not.
- Collecting and using information in a lawful, fair, and responsible way includes considering stricter standards when handling information about vulnerable populations and persons at risk. It also includes using stricter standards for particularly sensitive information. Potential impacts should be evaluated holistically. Information that does not appear especially sensitive on its own can become highly sensitive when combined with other available information. It can also become highly sensitive when viewed in context, which may require considering cultural, geographic, religious, or political circumstances.



Risk mitigation

- Ensures collection, use, and disclosure of sensitive data is based on legal authority – e.g. evaluate what laws allow you to collect, use and share information. This means find the law and cite it.
- Think about data that can be used discriminatorily. E.g.
 Geolocation data on its own may not seem sensitive but when
 paired with other data can be very sensitive/population based
 (religious communities) (needle exchanges)
- Provides guidance making ethical decisions to navigate risk in gray, unregulated areas like AI, automated decision making



*** DATA MINIMIZATION**

The minimum amount of information is collected, used, or shared to accomplish the stated purpose for collecting the information.



DATA MINIMIZATION



Implementation

- Collect only the minimum amount of information needed to accomplish a specific purpose.
- Minimize data use and disclosure by only allowing access to the minimum amount of information by the minimum number of people or organizations to accomplish a specific purpose.
- This includes utilizing de-identified or anonymous information when possible.
- Retain information only for the length of time that is necessary for its original purpose and applicable retention requirements.



Risk Mitigation

- Less data means less risk
 - How so?
 - Less to breach
 - Less to hack/ransomware
 - Less to protect
 - Less to search and produce for public records
 - Less data collection can translate to better data quality and integrity



PURPOSE LIMITATION

The reasons for gathering information are identified before it is collected. Use and disclosure is limited to what is reasonably necessary in relation to the specific reasons the information was collected.



PURPOSE LIMITATION



Implementation

- Specifically state the reasons for collecting information.
- Unless a person provides consent, the information should not be used or shared for purposes that are not reasonably necessary to, or compatible with, the original purpose for collecting the information.
- Examples of compatible purposes include public archiving, research, or disclosures required by law.



Risk Mitigation

- Forces you to be deliberate and think about what you are collecting
- Avoids data scope creep
- Avoids over collection of data

- Accountability
- Reduces liability legitimacy
- Privacy by design/privacy by default principles



TRANSPARENCY & ACCOUNTABILITY

- Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with under what circumstances.
- Accountability means being responsible and answerable for following data privacy laws and principles.



TRANSPARENCY & ACCOUNTABILITY



Implementation

- Provide notice that is clear, honest, and open about what information is collected, how it is used, and who it is shared with. When information is inappropriately used or disclosed, give timely notice to affected individuals.
- Ensure accountability for adherence to these principles, any applicable privacy laws, and the public's expectations for the appropriate use of personal information.
- Accountability includes creating and maintaining policies and other records to demonstrate compliance and appropriate information handling.
- It also includes processes for monitoring or auditing, receiving and responding to complaints, and redress for harmed individuals.



Risk Mitigation

- "Sunshine is the best disinfectant" ©
- Transparency also includes "plain language." Being clear about your intentions with data lessens the risk of confusion, deception, complaints.
- Accountability holds entities and employees to the standards set forth in transparent data policies. Everyone more likely to follow clear processes and procedures.
- Sets clear expectations for organizations, staff, public.



DUE DILIGENCE

Taking reasonable steps and exercising care before and after entering into an agreement or arrangement with a third party that includes sharing personal information.



DUE DILIGENCE



Implementation

Exercise due diligence when sharing information with third parties. Appropriate due diligence will vary based on the circumstances, but may include:

- Ensuring authority for the recipient to receive the information
- Evaluating whether sharing is consistent with the original purpose of collecting the information
- Requiring the third party to adhere to the same data use and security standards as the agency, including agency policies, these principles and applicable privacy laws
- Verifying and monitoring the third party's data use and security practices



Risk Mitigation

- Requires research/thoughtfulness before handing over data to third parties (this includes those in authority)
- Good contracts! (examples: indemnification, insurance, cybersecurity, limited lability, governing law, termination, warranty, pass through data security requirements, secure destruction of data, etc.)
- Monitor/audit System and Organization Controls (SOC)
- Reputation/reviews



❖ INDIVIDUAL PARTICIPATION

Give people control of their information when possible.



INDIVIDUAL PARTICIPATION



Implementation

- Involve people in the collection and management of their personal information whenever practicable and consistent with the government functions being performed. Individual participation may include processes to:
 - Provide, revoke, or manage consent
 - Opt-out or restrict collection or use
 - Access information
 - Request corrections to inaccurate information
 - Learn who information has been shared with
 - Timely response to requests for information



Risk Mitigation

- Creates records of informed consent and authorization
- Allows individuals some control over their data
- Provides direction to those handling data e.g. clear restrictions or sharing allowances
- Ensures more accurate, high-quality data (which reduces business risk of bad decisions based on bad data)
- Revocation processes "as easy to revoke as it is to consent"



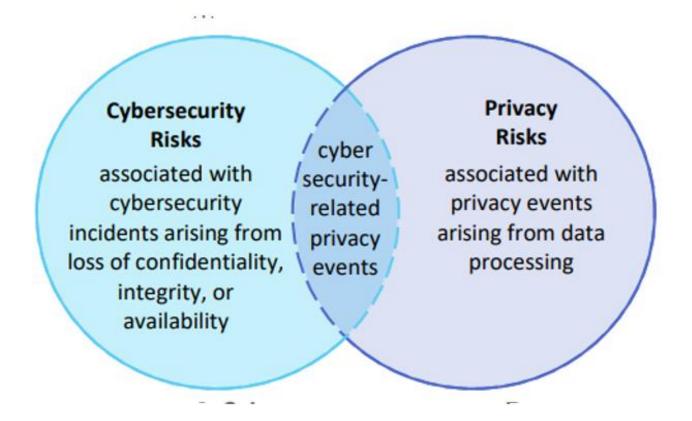
SECURITY

Appropriate administrative, technical, and physical security practices to protect the confidentiality, integrity, and accessibility of personal information.





Cybersecurity Relationship to Privacy



SECURITY



Implementation

• Establish, implement, and maintain reasonable security controls. Cybersecurity and non-technical controls must be appropriate to the amount and type of personal information being protected. Determining which security practices are reasonable includes considering what technology is available, the cost of implementation, and assessment of risk.



Risk Mitigation

- "Make the secure thing the easy thing"
- Secure data is protected data
- Protect against data breaches
 - Network infiltration; exfiltration of data
- Protect against ransomware
- Identify, detect, address vulnerabilities
- Internet/endpoint/cloud/application security



Just ask yourself does the adoption of _____ [fill in the blank privacy principle] reduce risk?

- Does the adoption of lawful, fair, and responsible data management reduce risk?
- Does the adoption of data minimization practices reduce risk?
- Does the adoption of transparent and accountable data management reduce risk?
- Does due diligence in selection of who and how you share your data with third parties reduce risk?
- Does allowing for individual participation in the data collection, use, and sharing process reduce risk?
- Does robust security for systems holding sensitive information reduce risk?





O P D P

https://watech.wa.gov/Privacy





P D P



Thank you!

privacy@watech.wa.gov

P D P