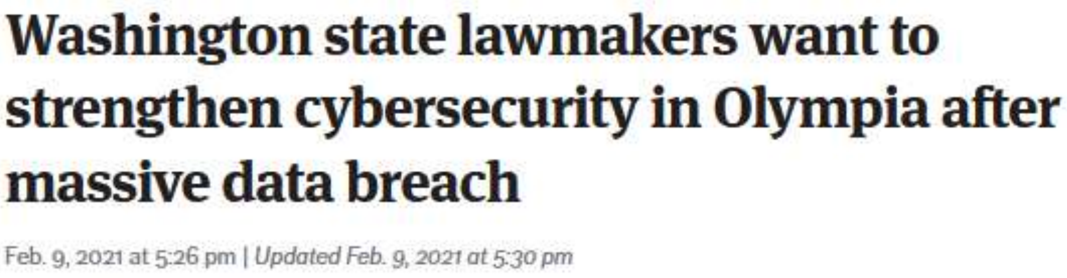
WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Implementation of Cybersecurity Legislation in Washington

Office of Privacy and Data Protection
NCSL Presentation
May 20, 2022

Background



Washington state lawmakers want to strengthen cybersecurity in Olympia after massive data breach

Feb. 9, 2021 at 5:26 pm | *Updated Feb. 9, 2021 at 5:30 pm*

ESSB 5432 – Concerning cybersecurity and data sharing in Washington state government

- OCS creation
- Catalog of services
- Incident response
- Independent security assessment
- Data sharing agreements

OCS created in statute

THE SEAL OF THE STATE OF WASHINGTON 1889
WaTech
Washington Technology Solutions
State Office of Cybersecurity

https://cybersecurity.wa.gov/

Catalog of Services

Report due to governor and legislature July 1, 2022

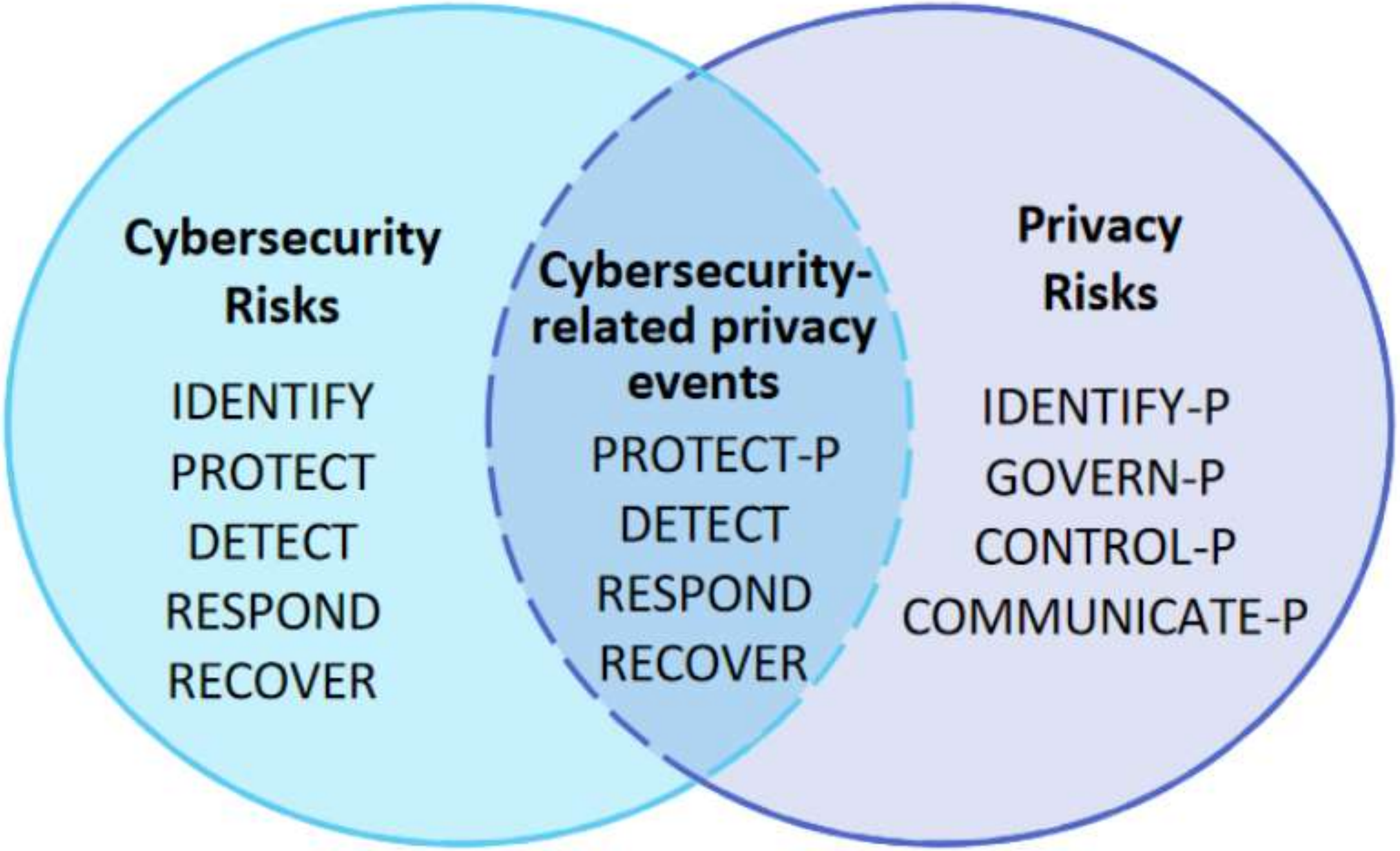
- Cybersecurity services that should be performed by OCS
- Security functions that should remain at agencies
- Catalog to be updated on a biennial basis

Service Areas:

- Endpoint Security
- Security Information and Event Management
- Vulnerability Management
- Risk & Compliance Management
- Application Security
- Data Security
- Security Incident Management
- Threat Detection & Intelligence
- Threat Hunting
- Network & Perimeter

O
P
D
P

Cybersecurity Incident Response



Source:

NIST Privacy Framework

OPDP

Section 4

The office of cybersecurity, in collaboration with the office of privacy and data protection and the office of the attorney general, shall:

- Research and examine existing best practices for
  - data governance,
  - data protection,
  - the sharing of data relating to cybersecurity, and
  - the protection of state and local governments' information technology systems and infrastructure
- including, but not limited to,
  - model terms for data-sharing contracts and
  - adherence to privacy principles.
- Report on findings and recommendations due 12/1/2021

Report Submitted December 1, 2021

Cybersecurity, Privacy and Data Sharing Agreements Best Practices Report

- Findings and recommendations related to:
  - Cybersecurity
  - Privacy
  - Data sharing agreements

Data Sharing Agreement Implementation Guidance

Sample DSA for defined extract or system access

Sample DSA for multiparty relationship with broad sharing

Misc. Privacy Recommendations

OPDP should:

- Develop additional training and awareness tools
- Tailor resources to address the greatest privacy risks
- Incorporate WSAPP in new resources, such as privacy impact assessments
- Promote workforce development
- Publish privacy impact assessment templates for major IT projects that involve personal information

Agencies should:

- Continue to invest in their privacy programs
- Designate privacy contacts, even if privacy is not that person's full-time job
- Make training mandatory for some or all staff
- Implement formal privacy policies that incorporate privacy principles

OPDP

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

O
P
D
P

Data Sharing Agreements

Other benefits

- Document all data flows
- Ensure appropriate protections to prevent incidents and misuse
- Outline responsibilities and mitigate impacts when an incident does occur
- Creates a gate to vet data sharing relationships

Identify – What is data sharing?

Making data available to third parties.

Types of sharing include:

- Data transmissions
- Data hosting
- System access

Functions include routine sharing necessary for an agency to perform core functions, such as sharing with:

- Contractors
- Service providers
- Other public agencies

Identify – Controls and processes

- Consider all ways third parties access information
- Log and track data sent outside of systems
- Build safeguards into existing processes
  - Contracting
  - Data product development
- Create common intake tools
- Develop approval requirements
- Policies to require data sharing agreements

OPDP

Implement – What is a DSA?

- Not defined in statute or OCIO policy
- Focus on appropriate data sharing language
- No requirement to have a document called a “Data Sharing Agreement”
- No requirement that DSA be a separate document

Implement – Flexibility required

- Not one, single version of model terms appropriate for all circumstances
- Consider:
  - Number of parties
  - Direction of sharing
  - Relationship between the parties
  - Method of sharing
  - Purpose of sharing
  - Frequency of sharing
  - Scope of sharing

Implement – Flexibility required

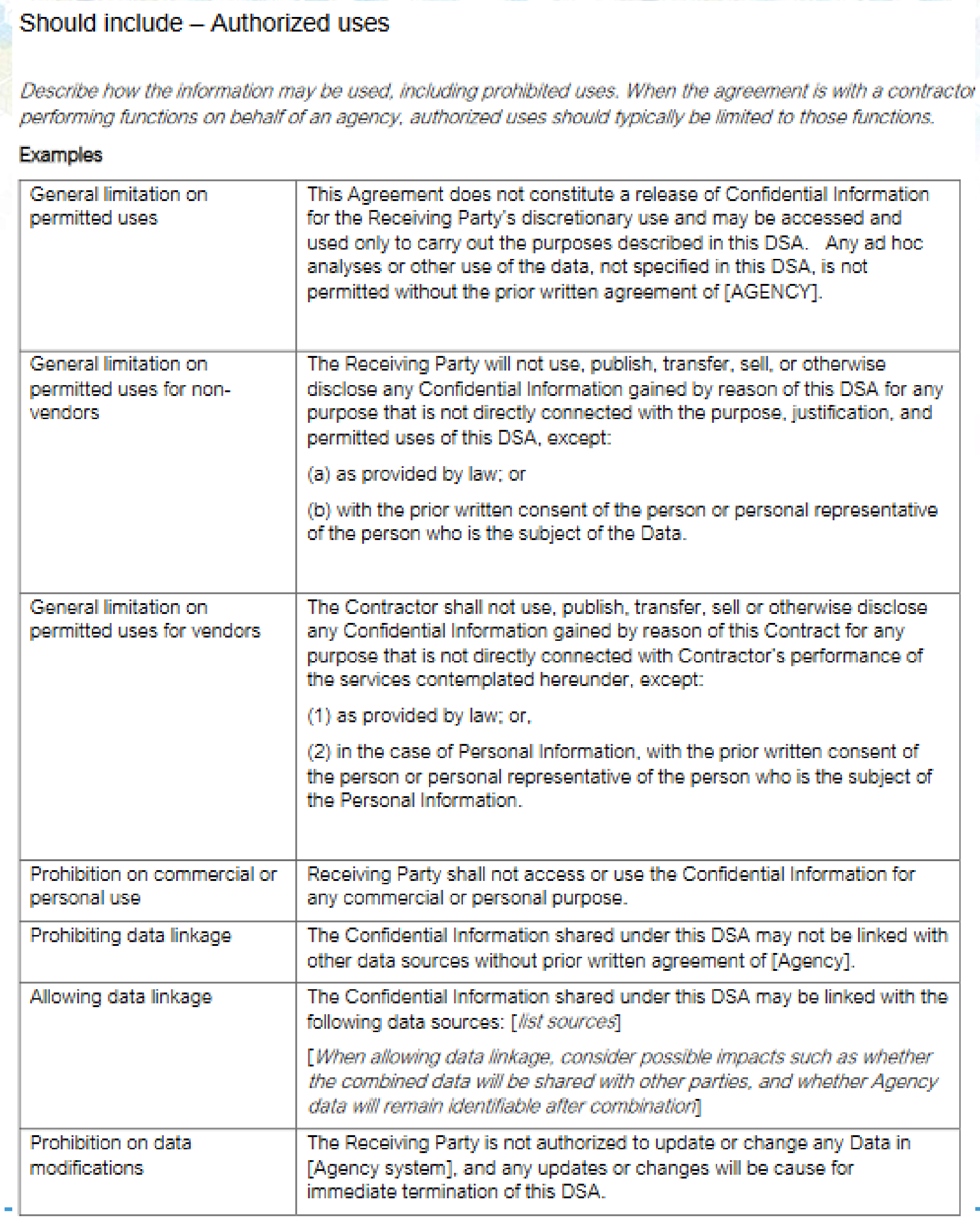
Flexible, not lackadaisical

Should Include	
Purpose and specific authority for sharing.	Backup requirements if applicable.
A description of the data, including classification.	Incident notification and response.
Authorized uses.	Monitoring and enforcement.
Authorized users or classes of users.	Awareness and/or training.
Protection of the data in transit if the arrangement involves transmission.	Compliance with additional relevant OCIO security requirements based on the type of data sharing.
Secure storage for data maintained outside the agency.	Any other requirements imposed by law, regulation, contract or policy.
Data disposal.	

Might Include
Term and termination.
Off-shore prohibition.
Cyber liability insurance.
Indemnification.
Third party requests.
Restrictions on disclosure or publication.
Other widely applicable contract terms.

Data Sharing Agreement Implementation Guidance

December 2021, v.1

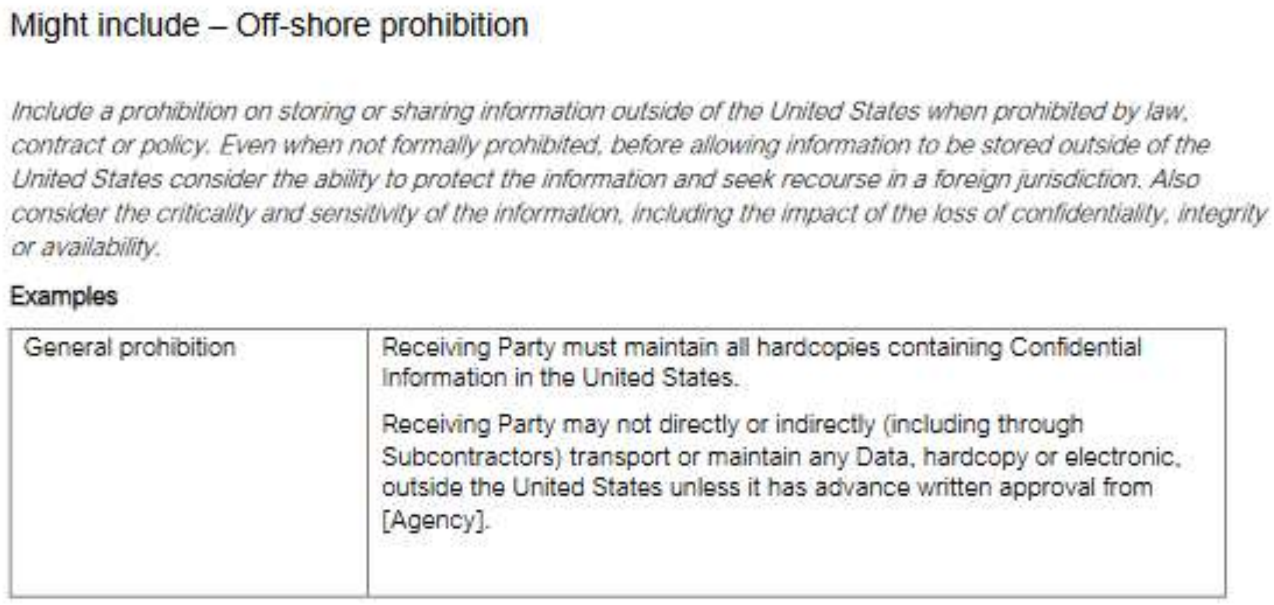


Should include – Authorized uses

Describe how the information may be used, including prohibited uses. When the agreement is with a contractor performing functions on behalf of an agency, authorized uses should typically be limited to those functions.

Examples

General limitation on permitted uses	This Agreement does not constitute a release of Confidential Information for the Receiving Party's discretionary use and may be accessed and used only to carry out the purposes described in this DSA. Any ad hoc analyses or other use of the data, not specified in this DSA, is not permitted without the prior written agreement of [AGENCY].
General limitation on permitted uses for non-vendors	The Receiving Party will not use, publish, transfer, sell, or otherwise disclose any Confidential Information gained by reason of this DSA for any purpose that is not directly connected with the purpose, justification, and permitted uses of this DSA, except: (a) as provided by law; or (b) with the prior written consent of the person or personal representative of the person who is the subject of the Data.
General limitation on permitted uses for vendors	The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with Contractor's performance of the services contemplated hereunder, except: (1) as provided by law; or, (2) in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information.
Prohibition on commercial or personal use	Receiving Party shall not access or use the Confidential Information for any commercial or personal purpose.
Prohibiting data linkage	The Confidential Information shared under this DSA may not be linked with other data sources without prior written agreement of [Agency].
Allowing data linkage	The Confidential Information shared under this DSA may be linked with the following data sources: [*list sources*] [*When allowing data linkage, consider possible impacts such as whether the combined data will be shared with other parties, and whether Agency data will remain identifiable after combination*]
Prohibition on data modifications	The Receiving Party is not authorized to update or change any Data in [Agency system], and any updates or changes will be cause for immediate termination of this DSA.



Might include – Off-shore prohibition

Include a prohibition on storing or sharing information outside of the United States when prohibited by law, contract or policy. Even when not formally prohibited, before allowing information to be stored outside of the United States consider the ability to protect the information and seek recourse in a foreign jurisdiction. Also consider the criticality and sensitivity of the information, including the impact of the loss of confidentiality, integrity or availability.

Examples

General prohibition	Receiving Party must maintain all hardcopies containing Confidential Information in the United States. Receiving Party may not directly or indirectly (including through Subcontractors) transport or maintain any Data, hardcopy or electronic, outside the United States unless it has advance written approval from [Agency].

Using implementation guidance

- For each type of term, there may be multiple appropriate terms or none.
- Be ready to add content and narrative.
- Some terms overlap – one contract clause can cover multiple concepts
- Only exercise flexibility when appropriate for specific relationships
- Only exercise flexibility when appropriate for specific terms

DSA Sample #1

Agreement for system access or pre-defined extract

- More appropriate for DSA when greater specificity is possible
- Includes alternative language for data sharing through system access transmitting data extract
- Contemplates sharing multiple types of information with one party
  - General requirements laid out in DSA, with new exhibits for each data sharing arrangement
- Includes sample data disposal certification document

DSA Sample #2

Overarching agreement for multi-party relationship

- More appropriate when there are multiple parties sharing with each other and/or the nature of the relationship makes specificity impossible
- Although more general, include at least purpose, authority and the types of information shared with as much detail as possible

Thank you

Questions?

privacy@watech.wa.gov

www.watech.wa.gov/privacy