Briefing: Data Stewardship Principles

Will Saunders, Chief Privacy Officer (acting) TSB Meeting September 2019

Background:

During the 2019 legislative session Senator Reuven Carlyle proposed SB5377, a bill which (if adopted) would have established common data stewardship principles and statutory minimum processes for agency sharing of data. Statutory changes are not within the authority of the Privacy Officer, but principles and best practices are.

The Office of Privacy and Data Protection is required by law to articulate privacy principles and best practices (RCW 43.105.369)

To date the Privacy Office has published guidance and advisory materials including:

- "Tips and Tools" for citizens and privacy pros
- "Privacy Guide" for citizens
- "Privacy Assessment" for the legislature
- "How to Start a Privacy Program" for state agencies
- "Privacy Modeling" an open-source issue-spotting app built with grant funds
- "Privacy Checklists" an open-source checklists tool to help privacy officers

Status and Actions to Date:

Draft principles are nearly ready for adoption and publication by the Privacy Office – see attached or download here.

Since the close of the legislative session, the Privacy Office has been working with stakeholders to develop a version of the bill's principles that could be broadly supported by agencies. To date the following agency stakeholder groups have discussed and commented on the principles presented here:

- Privacy Officers through the Privacy Working Group
- Contract Managers through the Interagency Data Sharing Agreements Group
- Open data advocates through the Open Data Advisory Group
- Enterprise Architects through the Statewide Enterprise Architecture Resource Team
- Chief Information Security Officers through the CISO Group

Planned next steps include:

1. Cleanup and publication on Privacy.wa.gov
2. Publication in the annual Privacy Assessment (October)
3. Presentation to Agency stakeholder groups (November)
4. Presentation to the legislature if desired (January)

Question for the Board:

Should the Chief Privacy Officer adopt the attached "Data Stewardship Principles" as best practices; and if so, how should the principles be presented to agency and external stakeholders?

Discussion:

- Agencies are looking for guidance on a common approach to data stewardship – a common set of bullet points to mention when setting up a program or facing the legislature
- Principles can inform rules, standards, policies or bills
- These principles are based on United Nations Development Group guidance on the use of Big Data. They are consistent with existing 1970's era US privacy law and current federal agency privacy programs. They are compatible with GDPR, but do not implement the full scope of European or California privacy rights.
- Principles have little or no mandatory authority; they are a nice starting place, but they don't require action by agencies.
- City of Seattle adopted privacy principles in 2015, but their approach was swamped by debate over surveillance cameras
- City of Portland adopted a similar set of Data Privacy and Information Protection principles in June 2019 as part of their inquiry into Automated Decision Systems

Conclusion:

The Privacy Office requests TSB members' commentary and recommendations on how to best leverage the authority of the Chief Privacy Officer to establish a common foundation for data stewardship among state agencies.

Point of Contact / Lead staff:

Will Saunders | **Chief Privacy Officer (*acting*)**
Office of Privacy & Data Protection (WaTech)
360.407.8693 d | 360.890.2580 m | Skype
Privacy.wa..gov | WaTech.wa.gov | ORCID

Data Stewardship Principles for Lawful, Fair and Responsible Use

Discussion draft September 5, 2019

Principle	Description	Mandate	Compliance
DATA RETENTION & MINIMIZATION	Data access, analysis or other use should be kept to the minimum amount necessary to fulfill its purpose. Any retention of data should have a legitimate and fair basis, including beyond the purposes for which access to the data was originally granted, to ensure that no extra or just-in-case data set is stored. Any data retention should be also considered in light of the potential risks, harms and benefits. The data should be permanently deleted upon conclusion of the time period needed to fulfill its purpose, unless its extended retention is justified as mentioned in this Section above. Any deletion of data should be done in an appropriate	• Consistent with the record retention schedules currently required by law, state agencies shall examine their data retention practices and retain personal information only as long as needed to carry out the purpose for which it was originally collected, or the minimum period required by law. (*Executive Order 16-01*)	• Have a data map (Checklist) • Follow Retention requirements • Consent in context • Review PII every 5 years
DUE DILIGENCE FOR THIRD PARTY COLLABORATORS	Third party collaborators engaging in data use should act in compliance with relevant laws, including privacy laws as well as the highest standards of confidentiality and moral and ethical conduct. Furthermore, third party collaborators' actions should adhere to the same principles as public agencies. It is recommended that a process of due diligence be conducted to evaluate the data practices of any potential third party collaborators. Legally binding agreements outlining parameters for data access and handling (e.g. data security, data formats, data transmission, fusion, analysis, validation, storage, retention, re-use, licensing, etc.) should be established to ensure reliable and secure access to data provided by third party collaborators	• State agencies shall notify the Chief Privacy Officer of the sale of any personally identifiable information or lists of individuals to third parties, except where such information has already been made available to the public. (*Executive Order 16-01*) • Legally binding agreements outlining parameters for data access and handling (e.g. data security, data formats, data transmission, fusion, analysis, validation, storage, retention, re-use, licensing, disposition, etc.) should be established to ensure reliable and secure access to data provided by third party collaborators.	• Document all data flows with Data Sharing agreements (checklist) • Report Data Sharing Agreements in contract management system (e.g. eCMS) • Audit data sharing agreement partners • Include data protection certifications such as SOC and PCI in procurements)
SENSITIVE DATA AND SENSITIVE CONTEXTS	Stricter standards of data protection should be employed while obtaining, accessing, collecting, analyzing or otherwise using data on vulnerable populations and persons at risk, children and young people, or any other sensitive data. It is important to consider that context can turn non-sensitive data into sensitive data. The context in which the data is used (e.g. cultural, geographic, religious, the political circumstances, etc.) may influence the effect of the data analysis on an individual(s) or group(s) of individuals, even if the data is not explicitly personal or sensitive.	• Policies must ensure that information regarding a person's immigration or citizenship status or place of birth shall not be collected, except as required by federal or state law or state agency policy; (*Exec Order 17-01*)	
DATA QUALITY AND ACCURACY	All data-related activities should be designed, carried out, reported and documented accurately. More specifically, data should be validated for accuracy, relevancy, sufficiency, integrity, completeness, usability, validity and coherence, and be kept up to date. Data quality should be carefully considered in light of the risks that the use of low quality data for decision-making can create for an individual(s) and group(s) of individuals.		

OPEN DATA, TRANSPARENCY AND ACCOUNTABILITY	Transparency is a critical element of accountability. Being transparent about data use (e.g. publishing data sets or publishing an organization's data use practices) is generally encouraged, but must be balanced against privacy, justice, and environmental stewardship. Except in cases where there is a legitimate reason not to do so, the existence, description, meaning, authorship, location, age and purpose of data use should be publicly disclosed and described in a clear and non-technical language suitable for a general audience. Open data is an important driver of innovation, transparency and accountability. Therefore, whenever possible, the data should be made open, unless there are legitimate reasons not to do so. Disclosure of personal information through public data should be avoided or carefully assessed for potential risks and harms.	• It is the intent of the legislature to encourage state and local governments to develop, store, and manage their public records and information in electronic formats to meet their missions and objectives. (*RCW 43.105.351*) • Agencies must develop, implement and maintain an Open Data Plan that outlines how the agency will routinely work to make open data publicly available. (*OCIO policy 187*) • To the extent possible, information must be collected directly from, and with the consent of, the individual who is the subject of the data. (*RCW 43.105.365*)	• Review data for possible publication (checklist) • Adopt and publish an open data plan (dashboard) • Follow metadata standards
DATA SECURITY	Data security is crucial in ensuring data privacy and data protection. Taking into account available technology and cost of implementation, robust technical and organizational safeguards and procedures (including efficient monitoring of data access and data breach notification procedures) should be implemented to ensure proper data management throughout the data lifecycle and prevent any unauthorized use, disclosure or breach of personal data. No de-identified data should knowingly and purposely be re-identified, unless there is a legitimate, lawful and fair basis. Data access should be limited to authorized personnel, based on the "need-to-know" principle. Personnel should undergo regular and systematic data privacy and data security trainings. Prior to data use, vulnerabilities of the security system (including data storage, way of transfer, etc.) should be assessed.	• Each agency will conduct an Information Technology Security Policy and Standards Compliance Audit at least once every three years. (OCIO policy 141) • Data Breach notification law	• Annual security assessment • Triennial audit • Security Design Review prior to deployment • Chief Information Security Officer on staff • Encryption in transit and at rest • De-identification / Pseudonymization • Privacy Impact Assesment (checklist)

This table of principles was developed by Privacy Office staff, based on the United Nations Development Group (UNDP) Guidance Note on Big Data (https://undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf), Articles 5 Principles of the General Data Protection Regulation (GDPR), and existing laws of Washington state.