Jurisdiction	Washington
Date	4/20/22
Law Firm	Polsinelli (https://www.polsinelli.com/)
Title, Name	Elizabeth (Liz) Harding, Shareholder Allison Krause, Associate
Contact Information	eharding@polsinelli.com, akrause@polsinelli.com

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the private sector at the present or in the near future? No.

ii. Does your country have a general law concerning protection of personal information in the public sector at the present or in the near future? No.

iii. Does your country have laws concerning protection of personal information which apply in individual (specific) sectors at the present or in the near future? (If yes, please describe outline.) No.

*There is no comprehensive law regarding the protection of personal information in Washington. However, in 2005, Washington enacted a data breach notification law, Wash. Rev. Code § 19.255.010, as amended (the "**WDBA**") that applies to private entities. The WDBA is similar to many other U.S. state laws regarding notification of data security breaches. All public agencies are subject to Wash. Rev. Code § 42.56.590 (the "**WGDBA**"), which contains the same principles and requirements as the WDBA. For purposes of this report the WDBA is inclusive of the WGDBA.*

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I..(please add a reply column as necessary,)

The title of the law ：*Wash. Rev. Code § 19.255.010 et seq., § 42.56.590*

URL:
https://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010
https://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.590

Enforcement status: *Enacted on July 24, 2005, amended on July 1, 2010, July 24, 2015 and March 1, 2020*

① The definition of "Personal Information"	*Personal information ("**PI**") includes an individual's first name or first initial and last name in combination with any one or more of the following items:* ***A**. Social Security Number* ***B**. Driver license number or government-issued ID number; or* ***C.** Account number or credit card number or debit card number in combination with any required security code, access code or password tat would permit access to an individual's financial account.* ***D**. Date of Birth* ***E**. Private key that is unique to an individual and that is used to authenticate or sign an electronic record;* ***F**. Student, military, or passport identification number;* ***G**. Health insurance policy number or health insurance identification number;* ***H**. Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or* ***I**. Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual.* *PI also includes information:* ***J**. Username or email address in combination with a password or security questions and answers that would permit access to an online account; and* ***K**. Any of the data elements or any combination of the data elements described in A-I*

	above, without the consumer's first name or first initial and last name if: (1) Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and (2) the data element or combination of data elements would enable a person to commit identity theft against a consumer. *It should be noted that PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.*
② The scope in which the law applies	*Any private or public entity which conducts business in WA that owns or licenses data that includes PI.*
③ The territorial scope	*The WDBA applies to data subjects located in Washington, and business operating outside of Washington must also comply with the law.*

ii. If there are any special instructions about the laws, please describe them.

Notification Obligations. *In the event of a data breach of PI, businesses must notify affected individuals. In addition, a business that is required to provide notification of a security breach of at least 500 Washington residents, must also notify the Attorney General of that breach within 30 days.*

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

The relevant provision is inapplicable.

(b) Data Quality Principle

While there is no provision specifying this principle, if an entity experiences an unauthorized acquisition of data that compromises the security, confidentiality or integrity of PI, such entity is required to notify the affected individuals, and if applicable the Attorney General in Washington.

(c) Purpose Specification Principle
The relevant provision is inapplicable.

(d) Use Limitation Principle
The relevant provision is inapplicable.

(e) Security Safeguards Principle
While there is no provision specifying this principle, if an entity experiences an unauthorized acquisition of data that compromises the security, confidentiality or integrity of PI, such entity is required to notify the affected individuals, and if applicable the Attorney General in Washington.

(f) Openness Principle
The relevant provision is inapplicable.

(g) Individual Participation Principle
Any consumer injured by a violation of the WDBA may institute a civil action to recover damages.

(h) Accountability Principle
The Attorney General may bring action on behalf of its state or its residents. In addition, if a business experiences a breach of unencrypted account or financial data, such entities can be liable to a financial institution for the cost of reissuing credit and debit cards.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.
None.

IV. Data Localization and Government Access

*While there is no rule regarding Data Localization and Government Access under the laws of Washington, US companies may theoretically be subject to US government surveillance laws, such as Section 702 of the Foreign Intelligence Surveillance Act ("**FISA 702**"), and National Security Letter requests issued by the FBI under Executive Order 12333 ("**EO 12333**" and together with FISA 702, "**US Government Surveillance Laws**"). US government commitments and policies*

restrict intelligence collection to what is required for foreign intelligence purposes and expressly prohibit the collection of information for other purposes, including commercial advantage.

*If violations of FISA 702 have occurred, individuals, including Japanese citizens and residents, may seek redress for said violations under several US statutes. An individual who has been subject to unlawful surveillance under FISA may seek damages, punitive damages, and attorney's fees against the individual who committed the violation. In addition, there is a separate private right of action provision under the Electronic Communications Privacy Act ("**ECPA**") for compensatory damages and attorney's fees against the government for FISA Section 702 violations. Further, individuals may also challenge unlawful FISA surveillance through the Administrative Procedures Act, 5 U.S.C. § 702 (2018), which allows individuals "suffering legal wrong because of" certain government conduct to seek a court order enjoining that conduct. Thus, as described above, Japanese citizens or residents, may seek redress for violations of FISA Section 702.*

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

None.