United States of America (Washington)

Existence or non-existence of a system for the protection of personal information	Although no comprehensive legislation currently exists, comprehensive privacy legislation has been discussed four times in the past and should be kept in mind. Representative laws applicable to individual fields include the following laws. ■Washington Revised Code §§ 19.255.010 and 42.56.590 (Hereinafter referred to as "Data Breach Notification Act"). - URL : https://app.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 March 1, 2020 - Target institutions: State or local agencies that own or license data containing personal information, and individuals or businesses operating in Washington State - Information covered:"Personal Information (PI)" The following are considered personal information (PI) if they meet any of the criteria below. However, information lawfully made available to the general public from federal, state, or local government records is not included. A. The combination of an individual's name or initials with their surname, along with one or more of the following data elements: (1) Social Security number or the last four digits of the Social Security number; (2) driver's license number or Washington ID card number, (3) account number, credit card number, debit card number, or any required security code, access code, password, or other number or information that allows access to an individual's financial account, (4) the complete date of birth, (5) the individual's unique private key, which is used to authenticate or sign electronic records; (6) student ID, military ID, passport ID number, (7) health insurance policy number or health insurance subscriber identification number, (8) any information relating to a consumer's medical history, mental or physical condition, or medical diagnosis or treatment by a healthcare professional, (9) biometric data generated by automated measurement of an individual's biological characteristics, such as fingerprints, voiceprints, eye retina, iris, or other unique biological patterns or characteristics used to identify a particular individual data. B. Username or e-mail address combined with a password or security question and answer that allows access to the online account C. The following cases, where the consumer's name or initials with their surname are not included, but any combination of the above data elements or those listed in (A): When the data elements or combinations thereof are not rendered unusable through encryption, redaction, or other means. When the data elements or combination of data elements would allow identity theft to be committed against the consumer ■Washington Revised Code §§ 19.375.020 and 40.26.020 (Hereinafter referred to as "Biometrics Act") - URL : https://app.leg.wa.gov/RCW/default.aspx?cite=19.375.020 https://app.leg.wa.gov/RCW/default.aspx?cite=40.26.020 - Enforcement status: effective July 23, 2017 - Target institutions: Any entity that owns, licenses, maintains, stores, supervises, collects, processes, or obtains personal information about Washington State citizens (including entities outside of Washington State) - Information covered: Biometric identifiers (such as fingerprints, voiceprints, retinal scans, iris scans, and other unique biological patterns or characteristics) are data generated by automatic measurements of an individual's biological features and used to identify specific individuals. This does not include photographs, video recordings, audio recordings, or data derived from them, nor does it include information collected, used, or stored under the Federal law 'Health Insurance Portability and Accountability Act. ■Uniform Health Care Information Act, Washington Revised Code Chapter 70.02 - URL : https://app.leg.wa.gov/rcw/default.aspx?cite=70.02 - Enforcement status: Enacted July 28, 1991; amended July 1, 2014 - Target institutions: Health care providers that collect, maintain, use, or possess health care information about Washington State residents - Information covered: Medical Information" (any care, service, or procedure provided by a health care provider to diagnose, treat, or maintain a patient's physical or mental condition, or to affect the structure or function of the human body)

<table>
<tr><td>Information that could serve as an indicator about the system for the protection of personal information</td><td>EU Sufficiency Certification*1: None
APEC's CBPR System*2: July 25, 2012 Participation</td></tr>
<tr><td>The obligations of businesses and other etities or rights of the individual comply with the eight principles of the OECD privacy guidelines*3</td><td>In the case of economies participating in the APEC CBPR system, for the private sector, it is not necessary to provide information on this item, since a certain degree of predictability for the individual regarding the risks associated with the provision of personal data to third parties located abroad is considered to be guaranteed to a certain degree. Therefore, it is not necessarily required to provide information regarding this matter.
However, since the above regulations are state laws, information related to this item is provided. Regarding the obligations of businesses or entities to comply with the OECD Privacy Guidelines' 8 Principles or the rights of individuals, they are as follows:

<table><tr><td>(1) Principle of collection restriction</td><td>Partially stipulated in the Biometrics Authentication Law.</td></tr><tr><td>(2) Principle of data content</td><td>The relevant provision is inapplicable.</td></tr><tr><td>(3) Principle of clarification of purpose</td><td>Partially stipulated in the Biometrics Authentication Law.</td></tr><tr><td>(4) Principle of Restrictions on Use</td><td>It is partially provided for in the Data Breach Notification Law and the Biometric Authentication Law.</td></tr><tr><td>(5) Principles of Safety and Protection</td><td>This is provided for in the Data Breach Notification Law, the Biometric Authentication Law, and the Unified Medical Information Law.</td></tr><tr><td>(6) Principle of Publicity</td><td>The relevant provision is inapplicable.</td></tr><tr><td>(7) Principle of Individual Participation</td><td>It is partially provided for in the Uniform Health Information Law.</td></tr><tr><td>(8) Principle of Accountability</td><td>This is provided for in the Data Breach Notification Law, the Biometric Authentication Law, and the Unified Medical Information Law.</td></tr></table></td></tr>
<tr><td>Other systems that may have a significant impact on the rights and interests of the individual</td><td>■Systems related to the obligation to preserve personal information intrastate, which may have a significant impact on the rights and interests of the individual.

■A system that imposes an obligation on businesses to cooperate with government information collection activities, which may have a significant impact on the rights and interests of the individual.</td></tr>
</table>

1. The countries or regions that have obtained the EU Sufficiency Certification are those countries or regions that have been determined by the European Commission to have an adequate level of data protection based on the GDPR or its predecessor, the Data Protection Directive, which is a system for the protection of personal information in the EU (EU Member States and Iceland, Norway and Liechtenstein, which are part of the European Economic Area), which the Commission has designated as countries or regions with systems for the protection of personal information that are deemed to have an equivalent level of protection to our country.
In this sense, the fact that a country or region has obtained EU adequacy certification constitutes "information that may serve as an indicator regarding the system for the protection of personal information".

2. As a prerequisite for participation in the APEC CBPR system, it is stipulated that, like our country, has legislation that conforms to the APEC Privacy Framework and has enforcement authorities to investigate and rectify complaints or issues that cannot be resolved by CBPR-certified businesses or accountability agents. Therefore, economies participating in the APEC CBPR system, like our coutry, have laws that conform to the APEC Privacy Framework and enforcement authorities to enforce such laws, thus generally expecting protection of personal information similar to that in our country.
In this sense, the fact that an economy participates in APEC's CBPR system constitutes "information that can be used as an indicator of a system for the protection of personal information". The APEC CBPR system covers the private sector.

3. The eight principles of the OECD Privacy Guidelines serve as fundamental principles referenced by OECD member countries as well as internationally in their efforts to protect personal information. They are used as global standard effectively when countries develop their personal information protection systems.

(Updated October 28, 2022)