United States of America (Federal)

Existence or non-existence of a system for the protection of personal information	There is no comprehensive law. Representative laws applicable to individual fields include the following laws ■Electronic Communications Privacy Act of 1986 (Hereinafter referred to as "ECPA") - URL：https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 - Enforcement status: Enacted on October 21, 1986 - Target institutions: Public sectors, including local governments, and private sectors that conduct electronic storage*1 of personal data - Targeted information: "Electronic communications"(the transmission of symbols, signals, texts, images, sounds, data, or information of any nature transmitted in whole or in part by wired or electronic systems) ■Gramm Leach Bliley Act (Hereinafter referred to as "GLBA") - URL：https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act - Enforcement status: Enacted on November 12, 1999 - Target institutions: Private financial institutions significantly engaged (significantly engaged) in the financial services industry - Information covered: "Non-Public Personal Information" (any information collected from customers through the provision of financial services) ■Health Insurance Portability and Accounting Act ((Hereinafter referred to as "HIPAA") - URL：https://www.cdc.gov/phlp/publications/topic/hipaa.html - Enforcement status: Enacted on August 21, 1996 - Target institutions: Public institutions (including local governments) and private institutions and private institutions - Information covered: "Protected Health Information" (information related to health status, provision of health care, and payment for health care that can be linked to an individual)
Information that could serve as an indicator about the system for the protection of personal information	EU Sufficiency Certification*2: None APEC's CBPR System*3: July 25, 2012 Participation
The obligations of businesses and other etities or rights of the individual comply with the eight principles of the OECD privacy guidelines*4	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. With regard to the public sector, the obligations of public sector entities or the rights of individuals corresponding to the eight principles of the OECD privacy guidelines are as follows:

(1) Principle of collection restriction	It is partially provided for in HIPAA.
(2) Principle of data content	The relevant provision is inapplicable
(3) Principle of clarification of purpose	The relevant provision is inapplicable
(4) Principle of Restrictions on Use	ECPA and HIPAA provide in part.
(5) Principles of Safety and Protection	It is partially provided for in HIPAA.
(6) Principle of Publicity	The relevant provision is inapplicable
(7) Principle of Individual Participation	It is partially provided for in HIPAA.

	(8) Principle of Accountability	The relevant provision is inapplicable
Other systems that may have a significant impact on the rights and interests of the individual	■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.	

1. 'Electronic storage' refers to the temporary, intermediate storage of communications incidental to electronic transmission and the storage of such communications by an electronic communications service for backup protection purposes.
(18 U.S.C. § 2511.)

2. 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".

3. 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.

4. 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.

[Items to be noted]
■Act on the Protection of Personal Data (Act No. 57 of 2003) (hereinafter referred to as the "Personal Data Protection Act"). The purpose of Article 28, Paragraph 2 of the Act on the Protection of Personal Information is not only to increase the predictability of risks associated with the provision of personal data to third parties in foreign countries to the individual concerned, but also to encourage business operators who provide personal data to third parties in foreign countries to be more aware than before of the business environment at the third parties in the foreign countries to which they provide the data.
The provision of personal data to a third party in a foreign country also includes the point of encouraging the business operator to be more aware of the business environment of the third party in the foreign country to which the personal data is provided.
In addition, the specific content of the information to be provided by the business operator to the individual in accordance with the said paragraph may vary depending on the individual case.
Therefore, confirmation of the system for the protection of personal data in a foreign country should be the responsibility of the business operator providing personal data to a third party in a foreign country, and the above reference information provided by the Committee should be referenced only as a supplement.

■The above reference information provided by the Committee is based on the results of the "Survey of Systems for the Protection of Personal Information in Foreign Countries" conducted by the Committee, and is based solely on information as of October 2021, when the survey was conducted. After the date of the survey, there may be changes in the system for the protection of personal information in foreign countries, and the content of information that should be provided to the individual by a business entity that provides personal data to a third party in a foreign country may have been changed.

■The above reference information provided by the Committee is based on the results of the "Survey of Systems for the Protection of Personal Information in Foreign Countries" conducted by the Committee. It should be noted that the investigation was conducted with limited scope regarding the applicable laws and regulations from the following perspective, and is not necessarily exhaustive. If an entity that provides personal data to a third party in a foreign country possesses relevant information other than the above reference information, such information must also be provided to the individual in accordance with Article 28, Paragraph 2 of the Act on the Protection of Personal Information and Article 17, Paragraph 2 of the Enforcement Regulations of the Act on the Protection of Personal Information (the Rules of the Personal Information Protection Commission, No. 3 of 2016). The information must also be provided to the person in question.

- The following laws and regulations shall be covered by the survey, which are listed as representative by the consignor or subcontractor for the above survey.
    - The laws on the protection of personal information applicable to specific sectors in foreign countries that do not have comprehensive legislation on the protection of personal information
    - Laws and regulations concerning the system related to the obligation to preserve personal information in the territory
    - Laws and regulations concerning a system imposing on businesses the obligation to cooperate with government information gathering activities
- With respect to laws and regulations concerning systems that impose an obligation on business operators to cooperate with government information collection activities, the survey shall cover systems in which foreign governments have access to personal information held by business operators for both or either criminal law enforcement purposes or national security purposes and in which the business operators are required under such laws and regulations to provide personal information to the foreign government. The survey shall cover those that are required by such laws and regulations to provide personal information to foreign governments.

(Updated January 25, 2022)