Republic of Korea

Existence of Systems for Protection of Personal Information	The following act exists as a comprehensive law: ■ Personal Information Protection Act - URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG - Enacted: Enacted September 30, 2011. Enacted in current form on August 5, 2020 - Relevant Institutions: Public sector institutions acting as "Personal Information Processors" (including local and regional governments) and private sector institutions.[1] - Relevant Information: The term "personal information" denotes any of the following information relating to a living individual: (i) information that identifies a particular individual by his or her full name, resident registration number, image, etc.; (ii) information which, even if by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual (in this case, information that is easily combinable is determined by reasonably taking into account factors such as the likelihood of obtaining other information, as well as the required time, cost, technology, etc.); or (iii) information under items (i) or (ii) above that through being pseudonymized, falls within "information that is unable to identify a specific person without first using or combining additional information in an attempt to restore it to its original form".
Information that may be an Indicator of Personal Information Protection Systems	EU adequacy decision[2]: None (however, Korea gained an initial decision from the European Commission on March 30, 2021.)

[1] "A public institution, legal person, organization, and/or individual that processes personal information directly or indirectly in order to operate the personal information files for work-related purposes."

[2] This committee designates the EU (EU member countries and Iceland, Norway, and Lichtenstein which comprise part of the European Economic Area) as a foreign country with personal information protection standards deemed at the same protection level as Japan's. The European Committee has concluded that countries and regions which have acquired an EU Adequacy Decision have adequate data protection standards based on the EU's GDPR, i.e., the personal information protection system and the GDPR's predecessor, the Data Protection Directive. Accordingly, those countries can generally be expected to have personal information protection on a par with Japan's. In this sense, a country or region which has acquired an EU Adequacy Decision can be considered as "information that may be an indicator of personal information protection systems."

<table>
<tr><td></td><td>APEC CBPR system : Participating as of June 2017</td></tr>
<tr><td>Businesses' Obligations and Individual Rights Compatible with OECD Privacy Guidelines' 8 Principles[4]</td><td>If an economy is a member of APEC's CBPR, then the ability of an individual to predict the risks associated with the provision of their personal data to an overseas private sector third party is considered to be somewhat guaranteed, and therefore the provision of information related to this item is not necessarily required.
Public sector agency obligations and individual rights compatible with the OECD Privacy Guidelines' 8 Principles are as follows:
<table>
<tr><td>1) Collection Limitation Principle</td><td>Stipulated in the aforementioned act.</td></tr>
<tr><td>2) Data Quality Principle</td><td>Stipulated in the aforementioned act.</td></tr>
<tr><td>3) Purpose Specification Principle</td><td>Stipulated in the aforementioned act.</td></tr>
<tr><td>4) Use Limitation Principle</td><td>Stipulated in the aforementioned act.</td></tr>
<tr><td>5) Security Principle</td><td>Stipulated in the aforementioned act.</td></tr>
<tr><td>6) Openness Principle</td><td>Stipulated in the aforementioned act.</td></tr>
<tr><td>7) Individual Participation Principle</td><td>Stipulated in the aforementioned act.</td></tr>
<tr><td>8) Accountability Principle</td><td>Stipulated in the aforementioned act.</td></tr>
</table></td></tr>
<tr><td>Other Systems Which May Significantly Affect Individual Rights and Interests</td><td>■ Systems which relate to the obligation to store personal information in-region and which may significantly affect individual rights and interests
—

■ Systems which require businesses to cooperate with government information gathering and which may significantly affect individual rights and interests</td></tr>
</table>

[3] The prerequisites for participation in APEC's CBPR system are that the economy has laws that conform to the APEC Privacy Framework and stipulate that the enforcement institution has the authority to investigate and rectify complaints and problems that cannot be resolved by the CBPR-certified business or accountability agent. Therefore, participating economies of the APEC's CBPR system, like Japan, are assumed to have laws compliant with the APEC's Privacy Framework and an enforcement body that enforces such laws. Hence, they can generally be expected to have personal information protection on a par with Japan's. In this sense, an economy's participation in APEC's CBPR system can be considered as "information that may be an indicator of personal information protection systems." Note that APEC's CBPR system applies to the private sector.

[4] OECD Privacy Guidelines' 8 Principles are the basic principles followed by OECD participating countries and are referenced for international efforts to protect personal information. The principles are used as the de facto global standard by countries when implementing personal information protection systems.

	—

Things to Keep in Mind:

- The aim of the Act on the Protection of Personal Information (Act 57 of 2003), Article 28, Paragraph 2, includes such points as increasing a person's ability to predict the risks associated with the provision of personal data to overseas third parties, as well as facilitating increased awareness among businesses that provide such personal data concerning their overseas third parties' business environment. Furthermore, the specific information which a business should provide to the individual based on the said paragraph may differ depending on the individual circumstances. Therefore, confirmation of overseas protection of personal information systems should be the responsibility of businesses that provide personal data to overseas third parties. The above reference information provided by this committee should be viewed simply as supplementary information.
- The above reference information provided by this committee is based on the results of the "Survey of Overseas Protection of Personal Information Systems" conducted and is solely based on information as of October 2021, when the survey was conducted by the committee. If overseas protection of personal information systems has been amended since that time, then the information which should be provided to the individual by businesses that provide personal data to overseas third parties may have changed.
- As the above reference information provided by this committee is based on the results of the "Survey of Overseas Protection of Personal Information Systems" conducted by the committee, the survey was limited in the laws it investigated from the below perspectives, and therefore it is not comprehensive. If a business that provides personal data to overseas third parties possesses related information other than the above reference information, then based on the Act on the Protection of Personal Information, Article 28, Paragraph 2, and the Enforcement Regulations for the Act on the Protection of Personal Information (Personal Information Protection Committee Regulations 3 of 2016), Article 17, Paragraph 2, the relevant information must be provided to the individual.
    - The contractors and subcontractors related to the above survey proffered the below laws as representative targets for the survey:
        - Laws related to the protection of personal information as applied in individual fields, in countries that do not have comprehensive laws for the protection of personal information
        - Laws related to systems requiring personal information to be stored in-region
        - Laws related to systems requiring businesses to cooperate with government information gathering
    - Laws related to systems requiring businesses to cooperate with government information gathering are systems which allow overseas governments to access personal information held by a business for the purpose of either enforcing the criminal code or

protecting national security, or both. Relevant laws which obligate businesses to provide personal information to overseas governments were targeted for the survey.

Matters occurring post November 2021

- The Republic of Korea obtained an EU adequacy decision on December 17, 2021.

(Revised March 30, 2022)