[Attachment]: System for the protection of personal information in foreign countries (excerpt from materials published by the Personal Information Protection Commission)

United States of America

[Personal information protection system]: Personal information is protected by the following acts: ・Electronic Communications Privacy Act of 1986 Target institutions: Public and private sectors that store personal data electronically Control subjects: Any symbol, signal, text, sound, data, or transmission of information transmitted by an electronic system. ・Gramm Leach Bliley Act Target institutions: Private financial institutions engaged in the financial services industry Control subjects: Any information collected from customers through the provision of financial services
[Information that can serve as an index for systems related to the protection of personal information]: ・Participating countries in the APEC CBPR system (*1) (joined on July 25, 2012)
[Other regulations that may seriously affect the rights and interests of the individual]: None

Republic of Singapore

[Personal information protection system]: Personal information is protected by the following acts ・Personal Data Protection Act (No.26 of 2012) Target institution: private sector Control subjects: Data from which an individual can be identified, either from the data or by combining the data with other information to which the organization, etc. has access. ・Public Sector (Governance) Act (No.5 of 2018) Target Institutions: Public Sector Control subjects: Anything in a form that can be communicated, analyzed or processed
[Information that can serve as an index for systems related to the protection of personal information]: ・Participating in APEC CBPR system (participated in February 2018)
[Other systems that may have a significant impact on the rights and interests of the individual]: There are the following systems that impose an obligation on businesses to cooperate with the government's information gathering activities. ・Criminal Procedure Code A police officer of a certain rank or higher may obtain information when he/she deems it necessary for conducting an investigation, interrogation, trial, or proceedings based on the Code of Criminal Procedure. The police offier may issue a “written order” asking them to submit information or to provide access to that information.

Hong Kong Special Administrative Region of the People's Republic of China

[Personal information protection system]: Personal information is protected by the following ordinance. ・Personal Data (Privacy) Ordinance Target institutions: Public and private sector data users (those who control the collection, retention, processing or use of data) Control subjects: Relates to a living individual, from which the identity of the individual can be ascertained, and access to or processing of such data is available.

[Information that can serve as an index for systems related to the protection of personal information]: None

Note, however, that obligations of business operators, etc. or rights of individuals corresponding to the eight principles of the OECD Privacy Guidelines (*2) are stipulated in the above laws and regulations. OECD Privacy Guideline 8 Principles (*2).

[Other systems that may have a significant impact on the rights and interests of the individual]:

There are following systems that impose an obligation on businesses to cooperate with the government's information gathering activities.

・The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (NSL)

Requirements for response to questions and submission of materials by National Security Department of Hong Kong Special Administrative Region ("Hong Kong" Government) Police when dealing with criminal cases endangering national security.

Republic of the Philippines

[Personal information protection system]:

Personal information is protected by following acts:

・Act Protecting Individual Personal Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes

Target institutions: public and private sector

Control subjects: Any information that reveals an individual's identity or allows an individual's identity to be ascertained by a company that holds such information, or, any information that can identify an individual when combined with other information

[Information that can serve as an index for systems related to the protection of personal information]: None

Note, however, that obligations of business operators and rights of individuals correspond to the eight principles of OECD Privacy Guidelines are stipulated in the above act.

[Other systems that may have a significant impact on the rights and interests of the individual]: None

Kingdom of Thailand

[Personal information protection system]:

Personal information is protected by the following acts

・Personal Data Protection Act

Target institutions: public and private sector

Control subject: Information that enables the identification of the natural person concerned

[Information that can serve as an index for systems related to the protection of personal information]: None

Note, however, that it is stipulated in the above act with the exception of when obligations of business operators, etc. and rights of individuals correspond to the eight principles of OECD Privacy Guidelines apply to Accountability Principle.

[Other systems that may have a significant impact on the rights and interests of the individual]:

There is a system that imposes an obligation on business operators to cooperate with government information gathering activities, which may cause a significant impact on the rights and interests of individuals:

・Special Case Investigation Act

Special Case Investigators are authorized to require private individuals to provide information, etc. for the purpose of investigating certain crimes that seriously affect national security, public order and morals, etc.

(*1) The APEC CBPR system is a system that certifies compliance with the APEC Privacy Principles

regarding the protection of cross-border personal data. Participating countries are premised on having laws that comply with the APEC Privacy Principles, as well as, having the authority to investigate and correct problems that cannot be resolved by CBPR certified businesses and their certification bodies. Therefore, likewise Japan, the economies participating in this system are expected to have the act that comply with privacy principles of APEC and have an executive body to enforce the act. As such, it can be expected that information is protected at the level equivalent to that of Japan, it applies to "information that can serve as an indicator for systems related to the protection of personal information."

(*2) The eight principles of OECD Privacy Guidelines are referenced not only by OECD member countries but also by international efforts to protect personal information. It is a de facto global standard that is referred to when each country establishes a personal information protection act.

The eight principles are as follows:

1. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

i) within a reasonable time;

ii) at a charge, if any, that is not excessive;

iii) in a reasonable manner; and

iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Revised on April 1, 2022