Hong Kong

Existence of Systems for Protection of Personal Information	The following ordinance exists as a comprehensive law: ■ Personal Data (Privacy) Ordinance (PDPO) - URL: https://www.elegislation.gov.hk/hk/cap486!en/en-zh-HantHant-HK.pdf?FROMCAPIINDEX=Y - Enacted: December 20th, 1996 - Relevant Institutions: "Data users" in the public and private sectors (individuals who manage the collection, retention, processing, or use of personal data alone or jointly with others) - Relevant Information: 1) "Data" that is directly or indirectly related to a living individual, 2) which can realistically confirm the individual's identity directly or indirectly, 3) and is in a format that can be realistically accessed or processed.
Information that may be an Indicator of Personal Information Protection Systems	EU Adequacy Decision[1]: None APEC CBPR System[2]: None

[1] 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>Businesses' Obligations and Individual Rights Compatible with OECD Privacy Guidelines' 8 Principles[3]</td><td>Obligations of businesses and rights of individuals based on the OECD Privacy Guidelines 8 Principles are as follows:<table>
<tr><td>1) Collection Limitation Principle</td><td>This is stipulated in the above law (including the Data Protection Principles in Table 1 of the PDPO).</td></tr>
<tr><td>2) Data Quality Principle</td><td>This is stipulated in the above law.</td></tr>
<tr><td>3) Purpose Specification Principle</td><td>This is stipulated in the above law.</td></tr>
<tr><td>4) Use Limitation Principle</td><td>This is stipulated in the above law.</td></tr>
<tr><td>5) Security Principle</td><td>This is stipulated in the above law.</td></tr>
<tr><td>6) Openness Principle</td><td>This is stipulated in the above law.</td></tr>
<tr><td>7) Individual Participation Principle</td><td>This is stipulated in the above law.</td></tr>
<tr><td>8) Accountability Principle</td><td>This is stipulated in the above law.</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>

[2] 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.

[3] 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.

	1) The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region or Hong Kong National Security Law (NSL) - Responses to inquiries and requests for submission of materials by the National Security Division of the Hong Kong Police, when handling criminal cases that endanger national security. - With regards to access of personal information held by private businesses, this law has no regulations on the following basic principles, for example: · Limitations and security safeguards for the handling of acquired information · Ensuring the transparency of data access · Remedies in case of infringement of rights due to illegal access

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.

(Updated: January 25th, 2022)