2013 Webinar Series
Taiwan
Data Privacy
Data Protection
September 12, 2013
Taiwan Personal Data Protection Laws

Dr. George Lin/ Managing Partner
Mr. Wei, Yang-Hung/ Partner

2013/9/12
Historical Background
Historical Background

- 1990/9/3 - R.O.C. Department of Justice began drafting our first personal data protection law.

- 1995/8/11 – Computer Processed Personal Data Protection Act (CPPDPA) was promulgated and signed into force by the President, this is the first personal data protection law ever promulgated in Taiwan.

- 2004/9/8 – R.O.C. Executive Yuan submitted the new draft of Personal Data Protection Act (PDPA) to the Legislative Yuan (Congress).
2010/4/10 – The new PDPA was approved by the Legislative Yuan, and the effectuating date of the new PDPA was authorized to be decided by the Executive Yuan.

2012/9/21 – Executive Yuan announced that the new PDPA would be effectuated on 2012/10/1. However, the effectuation of Art. 6 (highly sensitive personal data) and Art.54 (the duty of notification concerning the personal data gathered indirectly before the enforcement of the new PDPA) was excluded. As of today, the effectuation of the two articles is still pending for Executive Yuan’s further announcement.
Agenda

Scope of Personal Data

Personal Data
Scope of Personal Data

- According to previous CPPDPA, only “computer processed” personal data would be protected.

- According to the new PDPA: all personal information, including the name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical report, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities and other information which may be used to identify a natural person, both directly and indirectly. (Article 2)
Corporate Data is not protected, however, personal data contained in corporate data is still protected.

Foreign individual’s personal data is within the protection scope.

Personal Data from public source will still be protected (Article 19 I (7)). Collecting, processing and using of personal data from public source are generally allowed and no written consent from the data subject will be necessary. However, to protect the interest of the data subject, the collecting agency may not misuse such personal data for the purposes out of the collecting scope.
Highly Sensitive Personal Data

Medical treatment, genetic information, sexual life, health examination and criminal record could not be collected, processed or used, except for (a) when in accordance with law; (2) when it is necessary for the government agency to perform its duties or for the non-government agency to fulfill the legal obligation, and when there are proper security measures; (3) when the data subject has disclosed such information by himself, or when the information concerned has been publicized legally; or (4) when the personal information is collected, processed or used under certain methods by a government agency or an academic research institution based on the purpose of medical treatment, personal hygiene or crime prevention statistic and/or study (Article 6).
Highly Sensitive Personal Data

- **Forbidden use in principle**, too strict to some industries, ie. hospitals, life insurance companies. As of today, this article is still not effectuated, and the Department of Justice is considering adding (a) for the purpose of public interest; and (b) with data subject’s written consent as additional 2 exceptions to the highly sensitive personal data.
Scope of Regulated Parties

- According to previous CPPDPA, only government agencies and specified industries (i.e., credit reference and data processing agencies, hospital, school, telecommunication companies, financial institutions, media and other government designated industries) were regulated.

- According to the new PDPA, any Taiwan entity or individual within the territory, including government or private agencies, are regulated.
Scope of Regulated Parties

- Foreign entities (including subsidiaries of Taiwan entities) outside of the territory are not regulated, however, Taiwan entities (including foreign branch office of Taiwan entities), either governmental or private, gathering or processing personal data of Taiwan nationals abroad is still regulated (Article 2 (7), (8) and Article 51 II).

- Exception: (1) when an individual who collects, processes or uses personal information in the course of personal activity of a domestic nature; or (2) if the audio-visual information is collected, processed or used in public places or public activities and not associated with the other personal information (Article 51 I).
Agenda

Collection Process & Use of Personal Data
Conditions in Advance to Collect, Process and Use Personal Data

- **Specific Purpose** – may not misuse.

- Government Agencies:
  a. Within the *scope of job functions* provided by laws and regulations (ie. household registration);
  b. A *written consent* has been made by the data subject; or
  c. *No prejudice* to the rights and interest of the data subject.
Conditions in Advance to Collect, Process and Use Personal Data

- Private Agencies:
  a. **in accordance with the laws**;
  b. when there is a **contract or quasi-contract** between the subject and the agency;
  c. where the data subject has **disclosed such information by himself** or when the information **has been publicized legally**;
  d. where it is necessary for public interests on **statistics** or the purpose of **academic research** conducted by a research institution. The information may not lead to the identification of a certain person after the treatment of the provide or the disclosure of the collector (**de-identification**);
Conditions in Advance to Collect, Process and Use Personal Data

e. where a **written consent** has been made by the data subject;

f. where the **public interest** is involved; or

g. where the personal data is **obtained from publicly available resources**. However, if the processing or using of such personal data will be **prejudicial to the data subject’s compelling interest**, the collecting party may not collect, process or use such personal data.
Written Consent?

- Must be informed consent – after the notification duty is performed.
- May be in writing or in certified electronic signature.
- Consent in assumption – not allowed in new PDPA.
- Reverse written consent – not allowed by the Department of Justice.
- Consent through an Agent – Ok
Duty of Notification

When a governmental or private agency collects personal data, it has the mandatory duty to inform the data subject of,

a. The **name of the** government or private **agency**;

b. **Purpose** of collection;

c. **Classification** of the personal information;

d. Time period, area target and way of **the use of personal information**;

e. **Rights of the data subject** and ways to exercise them; (right to inquiry and request for review, making duplications, supplementing or correcting, discontinue using and the deletion of personal data)

f. The data subject’s **free discretion to providing his/her personal data** or not, and the influence to the data subject’s rights or interest if the data subject refuses to provide his/her personal data.
Duty of Notification

- Exemptions of the Notification Duty
  a. when in accordance with other laws;
  b. when the collection of personal data is necessary for the government agency to perform its official duties or the private agency to fulfill the legal obligation;
  c. when the notice will impair the government agency in performing its official duties;
  d. when the notice will impair the interests of a third party;
  e. when the data subject should have known the content of the notification already.
Duty of Notification

f. When data subject has **disclosed such information by himself** or when the information **has been publicized legally**;

g. When the **notification may not be made** to the subject matter or his legal representative;

h. When it is necessary for the **public interest in statistics or the purpose of academic research**. The information may not be used to identify a certain person after a treatment of the provider or the disclosure of the collector (**de-identification**); or

i. Personal data **collected by the mass media** for the purpose of news reporting on the basis of **public interest**.
Using of Personal Data

- Principle – within the specific purpose and misuse prohibited.

- Exceptions – Government Agencies
  a. Where in accordance with laws;
  b. Where it is for national security or to promote public interest;
  c. Where it is to prevent harm on the life, body, freedom or property of the data subject;
  d. Where it is to prevent harm to the rights and interests of other people;
Using of Personal Data

e. Where it is necessary for public interest in statistics or the purpose of academic research conducted by a government agency or an academic research institution (de-identification);

f. Where such use may benefit the data subject; or

g. A written consent of the data subject has been obtained.

Exemptions – Private Agencies

Basically the same as with the government agencies, except that in condition (b) national security, and the condition (f) (data subject’s interest) are removed.
Agenda

International Transfer of Personal Data
International Transmission of Personal Data

- Basically the same rules concerning the use of personal data applied.

- Specific restrictions – the authorities may restrict personal data transmitted abroad if:
  a. Where it involves major national interests;
  b. Where national treaty or agreement specifies otherwise;
  c. Where the country receiving personal information lacks proper regulations towards the protection of personal information and it might harm the rights and interest of the data subject; or
  d. Where international transmission of personal information is made through an indirect method in which the provisions of this Act may not be applicable.
International Transmission of Personal Data

Examples:

a. 2012/9/25 – NCC ordered that Taiwan telecommunication companies **may not transmit personal data to China**, because China still lacks due protection on personal data.

b. 2012/2/8 – FSC ordered that any kind of international outsourcing of financial institution’s financial business, including data processing, should be approved by FSC in advance, and subject to the continuous supervision of FSC. As of today, **no application for outsourcing of personal data processing to China has ever been approved** by FSC.
Duty of Data Security Requirements

- Should adopt **proper security measures** to prevent personal data from being stolen, altered, damaged, destroyed or disclosed.

- Proper security measures: (the Enforcement Rule of PDPA)
  
  a. Allocating management personnel and substantial resources;
  
  b. Defining the scope of personal information;
  
  c. Establishing the mechanism of risk evaluation and management of personal information;
  
  d. Establishing the mechanism of preventing, giving notice of, and responding to accidents;
  
  e. Establishing an internal management procedure of collecting, processing, and using personal information;
Duty of Data Security Requirements

f. Managing information security and personnel;
g. Promoting acknowledgement, education and training;
h. Managing facility security;
i. Establishing a mechanism of auditing information security;
j. Keeping records of the use, locus information and proof; and
k. Integrated persistent improvements on the security and maintenance of personal information.

- Duty of Alert: when the personal data is stolen, disclosed, illegally altered or infringed in other ways due to the violation of this Act, the agency should notify the data subject.
Government Inspection & Sanctions For Violations
Government Administrative Inspection

- The authorities may:
  
a. **Perform inspection** if it is necessary for the protection of personal data. The staffs of the inspected agencies should comply with the requests from the authorities to explain relevant personal data protection matters and to provide relevant documentation and records; and

b. **Detain or duplicate personal data or its files**, which may be confiscated or may be served as evidence. The owner or the holder of such personal data or its files should have the duty to surrender the same pursuant to the authorities’ requests.
Legal Responsibilities for the Violation of PDPA

- **Administrative Sanctions:**
  a. Violate this Act to collect, process or use personal data – NTD 50,000 to NTD 500,000 (around USD 1,700 to 17,000) fines.
  b. Violate the duty of notification or duty of data security requirements – NTD 20,000 to NTD 200,000 (around USD 700 to 7,000) fines.
  c. Violate authorities’ inspection requests – NTD 20,000 to NTD 200,000 (around USD 700 to USD 7,000) fines.
  d. In the meantime, the authorities may take **direct enforcement measures**, such as confiscation, deletion or destruction of personal data files, to enforce the PDPA.
  e. Other regulations concerning **specific industries**, such as financial institutions.
Legal Responsibilities for the Violation of PDPA

- Damage Compensations:
  - a. **Class action** allowed.
  - b. Strict liability for the governmental agencies, and the **liability for presumptive wrongs for private agencies**.
  - c. Monetary compensation for mental damages are allowed.
  - d. Consequential damages – NTD 500 to NTD 200,000 (around USD 17 to 7,000) for each plaintiff, and NTD 200 million (around USD 7 million) for one incident (may be higher if the violation benefits the liable party for more than NTD 200 million).
Legal Responsibilities for the Violation of PDPA

- Criminal Sanctions:
  a. Violate this Act to collect, process or use personal data – sentence of no more than 2 years of imprisonment, or a fine of no more than NTD 200,000, or both.
  b. Violate this Act to collect, process or use personal data, with the intention of making profits – sentence of no more than 5 years of imprisonment, and a fine of no more than NTD 1 million.
  c. Illegally changing or deleting personal data files, or by other illegal means to impede the accuracy of other people’s personal data files, and caused damages to others, with the intention of making profits or damaging other’s interests – sentence of no more than 5 years, or a fine of no more than NTD 1 million, or both.
Website: http://www.linandpartners.com.tw/en/content.htm
Email: Attorneys@linandpartners.com.tw