TAIWAN, CHINA

LAW

The former Computer Processed Personal Data Protection Law (CPPL) was renamed as the Personal Data Protection Law (PDPL) and amended on May 26, 2010. The PDPL became effective on October 1, 2012, except that the provisions relating to sensitive personal data and the notification obligation for personal data indirectly collected before the effectiveness of the PDPL remained ineffective. The government later proposed further amendment to these and other provisions, which passed legislative procedure and became effective on March 15, 2016.

DEFINITIONS

Definition of personal data

According to PDPL, personal data means:

- Name
- Date of birth
- ID card number
- Passport number
- Characteristics
- Fingerprints
- Marital status
- Family
- Education
- Occupation
- Medical record
- Medical treatment
- Genetic information
- Sexual life
- Health checks
- Criminal records
- Contact information
- Financial conditions
- Social activities
- Other information which may directly or indirectly be used to identify a living natural person

Definition of sensitive personal data

According to the PDPL, sensitive personal data means the personal data relating to medical records, medical treatments, genetic information, sex life, health checks and criminal records.
NATIONAL DATA PROTECTION AUTHORITY

In Taiwan, there is no single national data protection authority. The various ministries and city / county governments serve as the competent authorities.

REGISTRATION

Unlike the CPPL, there is no need to register with any authorities for the collection, processing, usage and international transfer of personal data under the PDPL.

DATA PROTECTION OFFICERS

There is no requirement in Taiwan for the data controller to appoint a data protection officer. However, if the data controller is a government agency, a specific person should be appointed to be in charge of the security maintenance measures.

COLLECTION & PROCESSING

Under the PDPL, the data controller should not collect or process personal data unless there is specific purpose and should comply with one of the following conditions:

- Where collection / processing is explicitly stipulated by law
- Where there is a contract or quasi contract between the data controller and the data subject and there is proper security measures in place
- Where the data subject has him/herself disclosed such data to the public or where the data has been publicized legally
- Where it is necessary for public interest on statistics or the purpose of academic research conducted by a research institution. The data may not lead to the identification of a certain person after the treatment of the provider or by the disclosure of the collector
- Where consent has been given by the data subject (which may be assumed under certain circumstances where the data controller has explicitly informed the data subject of the information required by the PDPL, and the data subject has provided his/her personal data and has not expressed his / her rejection. Even so, the data controller has the burden of proof to show valid consent)
- Where it is necessary to enhance the public interest
- Where the personal data is obtained from publicly available sources, except that where the vital interest of the data subject requires more protection and the prohibition of the processing or usage of such personal information
- Where there is no infringement on the rights of interests of the data subject

Except for the exemptions stipulated in the PDPL (eg, if it is explicitly stipulated by law that the provision of such information is not required, or if the data subject is fully aware of the contents of the notice, or if it is not profit-seeking purpose and it is obviously not detrimental to the data subject), the data controller is permitted to collect and process personal data only if the data controller unambiguously informs the data subject of the following information prior to or upon the collection:

- Data controller’s name
- Purpose(s) for collecting personal data
- Categories of personal data
- Period, area, recipients and means of using the data
- The data subject’s rights and the methods by which the data subject may exercise those rights in accordance with the PDPL, and
- Where the data subject has the right to choose whether or not to provide the data, the consequences of not providing the data

The information collected should in principle only be used for the purpose notified and not for any other purpose unless falling within any of the exceptional circumstances as set forth in the PDPL (eg, where consent has been given by the data subject, or where it is beneficial to the rights or interests of the data subject).
In addition, the Employment Service Act and its Enforcement Rules require that an employer shall not request a job seeker or an employee to provide his / her privacy information which is unrelated to his/her employment. Such privacy information includes physiological information, psychological information and personal life information. When an employer asks a job seeker or an employee to provide his / her privacy information, the personal interest of the data subject should be respected; the request should not exceed necessary scope of specific purposes based on economic demand or public interest, and should have just and reasonable connection with the specific purposes.

As to sensitive personal data, its collection, processing or usage (including international transfer) is prohibited unless any of the statutory conditions is met, which include the circumstances where written consent of the data subject has been obtained (except that it exceeds the necessary scope of specific purposes, or other laws otherwise provide for, or the consent is contrary to his / her free will), or where the data subject has him / herself disclosed such data to the public or the data has been publicized legally.

**TRANSFER**

The central competent authority may restrict the international transfer of personal data by the data controller which is not a government agency in the following circumstances:

- Where it involves major national interests
- Where an international treaty or agreement specifies otherwise
- Where the country receiving personal data lacks proper regulations that protect personal data and that might harm the rights and interests of the data subject
- Where the international transfer of personal data is made to a third country through an indirect method in order to evade the provisions of the PDPL

**SECURITY**

Data controllers should adopt proper security measures (both technical and organizational) to prevent personal data from being stolen, altered, damaged, destroyed or disclosed.

The central competent authority may request the data controller which is a non-government agency to set up a plan for the security measures of the personal data file or the disposal measures for the personal data after termination of business.

**BREACH NOTIFICATION**

Where the personal data is stolen, disclosed, altered or infringed in other ways due to the violation of the PDPL, the data controller should notify the data subject after due inquiry.

**ENFORCEMENT**

Under the PDPL, the competent authority may perform an inspection, if it is necessary for the examination of the security measures of data files, of the disposal measures after termination of business, the limitation of international transfer, or other routine business, or if the PDPL may be violated. Those who perform the inspection may ask the data controller to provide a necessary explanation, take cooperative measures, or provide relevant evidence.

When the competent authority conducts such an inspection, it may seize or duplicate the personal data and files that may be confiscated or may be used as evidence. The owner, holder or keeper of the data or files should surrender them upon request.

In addition, a breach of the PDPL may be subject to criminal sanctions (if for a profit-seeking purpose), administrative fines, and civil compensation (collective action is permitted).

**ELECTRONIC MARKETING**

The PDPL applies to electronic marketing in the same way as to other marketing. Within the necessary scope of specific purposes of data collection, the data controller may use personal data for marketing. However, when the data subject refuses the marketing (a right to ‘opt out’), the data controller should cease using such personal data for marketing. In addition, when making the first
marketing, the data controller should bear the costs to provide the data subject with the means to refuse marketing.

ONLINE PRIVACY

There is no special law or regulation applicable to online privacy. The PDPL applies to online and physical world in the same manner. As a result, online unique issues are not specifically addressed.

KEY CONTACTS

Formosa Transnational Attorneys at Law
www.taiwanlaw.com/

Chun-yih Cheng
Senior Partner
Formosa Transnational Attorneys at Law
T +886 2 27557366 Ext 158
chun-yih.cheng@taiwanlaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization’s level of data protection maturity.
Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.