DATA PROTECTION LAWS OF THE WORLD

Taiwan

DLA PIPER

TAIWAN

Last modified 18 December 2023

LAW

The Taiwan Personal Data Protection Act (“**PDPA**”) as most recently amended on May 31, 2023 and the Enforcement Rules of the Personal Data Protection Act (“**Enforcement Rules**”) as most recently amended on March 2, 2016.

DEFINITIONS

Definition of personal data

The PDPA defines “personal data” as the name, date of birth, identification card number, passport number, special traits, fingerprints, marital status, family, education, profession, medical history, medical treatment, genetic information, sexual life (including sexual orientation), health examination, criminal record, contact information, financial condition, and social activities of a natural person, as well as other data by which such person may be directly or indirectly identified.

Definition of sensitive personal data

The PDPA defines “sensitive personal data” as medical records, medical treatment, genetic information, sexual life (including sexual orientation) and health examination and criminal records.

NATIONAL DATA PROTECTION AUTHORITY

Currently, the regulatory body with overall responsibility for data protection is the National Development Council ("**NDC** ”). However, according to the May 31, 2023 amendment of the PDPA, the NDC is expected to be replaced by an independent data protection authority (i.e. the Personal Data Protection Commission). This amendment has not been effective yet and its effective date remains uncertain as of date.

In addition, the authority with jurisdiction over the relevant data collector has primary enforcement responsibility (e.g. the Financial Supervisory Commission has the primary enforcement responsibility *vis-á-vis* financial institutions).

REGISTRATION

Taiwan does not have a registration system for personal data protection.

DATA PROTECTION OFFICERS

The PDPA does not impose a general requirement to have a data protection officer. However, there are industry specific regulations in certain industries (such financial institutions or airlines) requiring personnel to handle personal data protection matters.

COLLECTION & PROCESSING

Under the PDPA, in order to collect, process and use personal data, the data collector is required to give the data subject a privacy notice at the time the data subject’s personal data is first collected. Such privacy notice is required, *inter alia,* to contain:

- the name of the data collector;
- the purpose of collection;
- classification of personal data to be collected;
- time period for the use, geographical area of the use, recipients of the data and the manner of using personal data;
- the rights of the data subject to request to review his / her personal data, to make copies of such personal data, to supplement or correct such personal data, to discontinue collection, processing or use of personal data or to delete such personal data, together with the manner in which the data subject makes such requests; and
- the impact on the data subject’s rights and interests if the data subject chooses not to provide his / her personal data.

As long as the privacy notice is given when the personal data is first collected, and the privacy notice meets the content requirements set out in the PDPA, the privacy notice is by itself considered sufficient (i.e. consent is not required). This is unless sensitive personal data is collected, in which case the data subject’s consent is required.

TRANSFER

The privacy notice to data subjects must set out the extent to which personal data will be transferred to others.

Cross-border transmissions of personal data are regulated by the PDPA. The Taiwan authorities may restrict the cross-border transmission and use of personal data in the following circumstances:

- when a substantial interest of Taiwan is at stake;
- as provided under an international treaty or agreement (as at December 10, 2021, there are no such treaties or agreements in place);
- when the receiving country lacks proper laws or regulations adequately to protect personal data or where infringement of the rights and interests of the data subject is threatened; or
- the purpose of the transfer is to evade the application of the PDPA.

The Taiwan National Communications Commission (NCC) issued an order in 2012 prohibiting communications enterprises from transferring subscribers’ personal data to mainland China; the Ministry of Health and Welfare issued an order in 2022 prohibiting social worker offices from transferring data subjects’ personal data to mainland China; and the Ministry of Labor issued an order in 2023 prohibiting private employment services institutions and employment service agencies for people with disabilities from transferring data subjects’ personal data to mainland China, all on the grounds that the personal data protection laws in mainland China are still inadequate. As at December 18, 2023, there are no other restrictions or prohibitions on the cross-border transfers to any other country / area.

SECURITY

A data collector is required to adopt proper security measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed.

In addition, the relevant competent authority at the central government level may designate certain data collectors for setting up plans of security measures for personal data files or the disposal measures for personal data after termination of business. As at December 18, 2023, industry specific guidelines governing the plan of security measures for personal data files have been promulgated for many industries, including for financial institutions, human resources recruitment business, hospitals, manufacturers, and others.

BREACH NOTIFICATION

Upon a data breach (which is not defined under the PDPA, however, from a Taiwan law perspective, such would mean where a data subject’s personal data is accessed, taken, revealed, leaked, changed or otherwise infringed on by any unauthorized person or entity or in any unauthorized manner), the data collector is required to promptly notify the data subject of:

- the fact of the infringement;
- the measures the data collector has taken to respond to such infringement; and
- the contact information of the data collector.

No threshold has been provided for when such notice has to be given to the affected data subjects. It is understood that so long as personal data is stolen, disclosed, altered or otherwise infringed on, such notice has to be promptly given.

The notice may be made orally, by written document, telephone, text message, email, facsimile, electronic record, or in another manner which the data subject can receive such notice. If the cost of notifying each data subject is “too high”, such notice may be made via the internet or news media.

In addition, data collectors in certain industries (e.g. travel agents, financial institutions) are required to report to their respective industry regulator and, where it is required to do so, the report to the industry regulator needs to include:

- the fact that personal data may have been compromised;
- the measures the data collector has taken to respond to such compromise (including evidence that the data collector has notified the affected individuals);
- the investigation by the data collector (or any outside forensic firm) as to how the data breach occurred;
- the preventive measure(s) the data collector will take to prevent recurrence of data breach in the future; and
- any other information that the industry regulator may require on a case-by-case basis.

Also, between 2021 and 2023, steps were taken by the Taiwan authorities to expand the material data breach reporting obligations of, *inter alia*, security service providers, pawnshops, travel agents and financial institutions by (i) requiring such enterprises to report material data breaches to the relevant industry competent authority within a specified period (e.g. 72 hours) and / or (ii) requiring such competent authorities to further report such breach to the NDC within 72 hours of becoming aware of the breach. Such steps are now being implemented or will shortly become effective. Also, the term “material data breach”, subject to the relevant regulations, in general means a situation where personal data is stolen, altered, damaged, destroyed or disclosed, and such will endanger the normal business of the data collector, or the rights and interests of a large number of data subjects (“large” has not been defined).

ENFORCEMENT

In addition to civil damages, violations of the PDPA, depending on the specific violation, are also subject to administrative sanctions and criminal sanctions and, in some cases, imprisonment.

Civil damages

If a data collector intentionally or negligently violates any provision of the PDPA and such violation causes illegal collection, processing or use of personal data or other infringement to a data subject, the data collector is liable to compensate the data subject for the damages suffered. Compensation may be both monetary and in the form of corrective measures (e.g. to rectify damage to the data subject’s reputation).

Where the victims may not have access to or cannot provide evidence for the amount of actual damage, the minimum amount is NT$ 500 (approx. US$ 18 as at December 10, 2021) and the maximum is NT$ 20,000 (approx. US$ 690 as at December 10, 2021) per violation / per injured party depending on the severity of the infringement. In the case of class actions, the aggregate total compensation to the class as a whole is limited to NT$ 200,000,000 (approx. US$ 6,900,000 as at December 10, 2021). However, one should not necessarily rely on these limits because the maxima do not apply if it can be proven that a higher amount is appropriate. Furthermore, the limits may be circumvented by resorting to general causes of action in tort over and above the specific statutory cause of action created by the PDPA.

Administrative sanctions

A regulatory body may impose administrative fines on a data collector in violation of the PDPA ranging from NT$ 20,000 (approx. US$ 690 as at December 10, 2021) to NT$ 500,000 (approx. US$ 17,300 as at December 10, 2021) per violation. These administrative fines may be imposed repeatedly until the violation is cured. The May 31, 2023 amendment of the PDPA increases the administrative sanctions on a data collector for its violation of data security obligations to up to NT$15,000,000 (approx. US$ 483,900 as at December 18, 2023), and such increase came into effect on June 2, 2023.

Also, the representative, managers or other persons having authority of the data collector which violates the PDPA are subject to the same administrative fines as the data collector itself, unless it is proven that the relevant representative, manager or other person having authority had properly performed his / her duties. There is no definition of representative, manager or other person having authority but generally such terms are understood to refer to the chairman and the general manager of the company.

Criminal sanctions

A person who, with the intention to gain “benefit” for themself or a third party or to “harm” the interests of others, violates certain requirements as set out in the PDPA or conducts a prohibited cross-border transfer of personal data may be punished by up to five years’ imprisonment and / or fines of up to NT$ 1,000,000 (approx. US$ 35,000 as at December 10, 2021). In addition, the acquisition, dissemination, alteration, compromise of the accuracy of, or deletion of personal data with the intent to gain “benefit” for themself or a third party or to “harm” the interests of others, in circumstances which is sufficient to cause damage to others, may also be punished by imprisonment for up to five years and / or fines of up to NT$ 1,000,000 (approx. US$ 35,000 as at December 10, 2021).

ELECTRONIC MARKETING

If a data collector wishes to use a data subject’s personal data for the purpose of direct marketing whether electronic or otherwise, such data collector is required to give the data subject a privacy notice (see Collection and Processing).

If a data subject requests the data controller to cease direct marketing, the data collector must stop using the data subject’s personal data for marketing.

In this regard, when a data collector uses personal data of a data subject to conduct marketing for the first time, the data collector must advise the data subject that they have the right to require cessation of the marketing and provide the data subject with information as to how to exercise such right. Also, the data collector must bear the cost of the first cessation request (e.g. by providing a toll-free line to call or a stamped pre-addressed envelope for return mail).

ONLINE PRIVACY

Although the PDPA does not specifically regulate online privacy, cookies and location data could be considered as social activities of a natural person by which such person may be directly or indirectly identified, as such the PDPA may apply to online privacy.

KEY CONTACTS

Russin & Vecchi
www.rvlaw.ru/taipei

Phoebe Yu
Partner
Russin & Vecchi
T +886-2-2713-6110
pyu@russinvecchi.com.tw

Helen Wang
Associate
Russin & Vecchi
T +886-2-2713-6110
hwang@russinvecchi.com.tw

DATA PRIVACY TOOL

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