GETTING THE DEAL THROUGH

Data Protection & Privacy

in 26 jurisdictions worldwide

2014

Contributing editor: Rosemary P Jay

Published by
Getting the Deal Through
in association with:

Adams & Adams

Arzinger

Coelho Ribeiro e Associados

Com advokatbyrå

Drew & Napier LLC

ELIG, Attorneys-at-Law

Gilbert + Tobin

Heenan Blaikie LLP

Hoffmann Liebs Fritsch & Partner

Hunton & Williams LLP

Ichay & Mullenex Avocats

Iriarte & Asociados

Jayaram & Jayaram

Laux Lawyers, Attorneys-at-Law

Lee and Li, Attorneys-at-Law

Lexing Spain

Lorenz International Lawyers

Matheson

MNKS

Nagashima Ohno & Tsunematsu

Olivares & Cia

Panetta & Associati Studio Legale

Pinheiro Neto Advogados

Preslmayr Rechtsanwälte OG

Yoon & Yang LLC

GETTING THE DEAL THROUGH

Data Protection & Privacy 2014

Contributing editor
Rosemary P Jay
Hunton & Williams

Publisher
Gideon Roberton

Business development managers
Alan Lee
George Ingledew
Dan White

Account manager
Megan Friedman

Trainee account managers
Cady Atkinson, Joseph Rush, Dominique Destrée and Emma Chowdhury

Media coordinator
Parween Bains

Administrative coordinator
Sophie Hickey

Trainee research coordinator
Robin Synnot

Marketing manager (subscriptions)
Rachel Nurse
subscriptions@gettingthedealthrough.com

Head of editorial production
Adam Myers

Production coordinator
Lydia Gerges

Senior production editor
Jonathan Cowie

Subeditor
Davet Hyland

Director
Callum Campbell

Managing director
Richard Davey

Data Protection & Privacy 2014
Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910
© Law Business Research Ltd 2013
No photocopying: copyright licences do not apply.
First published 2012
Second edition

ISSN 2051-1280

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of September 2013, be advised that this is a developing area.

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Law Business Research

CONTENTS

Taiwan

Ken-Ying Tseng and Rebecca Hsiao

Lee and Li, Attorneys-at-Law

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The collection, processing and use of personal data by regulated entities were subject to the Computer-processed Personal Data Protection Act (CPDPA) and its Enforcement Rules promulgated by the Ministry of Justice (MoJ). Regulated entities include all government agencies and the following entities in the private sector:

- credit investigation agents and entities or individuals whose main business is the collection of personal data;
- hospitals;
- schools;
- telecommunications businesses;
- banks and other financial entities;
- securities businesses;
- insurance companies;
- publishing and broadcasting companies; and
- any other entities designated by the competent authorities.

On 27 April 2010, the legislature passed a bill to amend and rename the CPDPA the 'Personal Data Protection Act' (PDPA). On 26 May 2010, the registration requirements under the CPDPA were abolished along with the president's promulgation of the PDPA. Other provisions (except for articles 6 and 54, explained below) under the PDPA and the MoJ's amended Enforcement Rules took effect on 1 October 2012 and apply to anyone who collects, processes or uses personal data.

Article 6 of the PDPA prohibits the collection, processing and use of sensitive data, unless any exemption condition is met. Since the exemption conditions are too limited to meet certain industries' needs, the Executive Yuan has proposed a draft bill to amend article 6 to include other exemption conditions.

Article 54 of the PDPA requires that, within one year of the effective date of the PDPA, data owners must notify data subjects of the notification information under the PDPA, if the data owners had obtained the data subjects' personal data indirectly before the effective date of the PDPA. Considering that certain industries that own a large quantity of personal data are not capable of meeting the notification requirement within the one-year period, the Executive Yuan has proposed a draft bill to amend article 54 so that data owners must meet the notification requirement no later than the first time they use such personal data to contact the data subjects. The draft bill is pending the legislature's reading.

The PDPA is a general law regulating the collection, processing and use of personal data. If there is any special law regulating the collection, processing and use of personal data, the special law should apply.

Under the PDPA, data owners are referred to as government agencies and non-government agencies (private sector). The PDPA imposes civil and criminal liabilities on government agencies, and imposes civil, criminal and administrative liabilities on non-government agencies if they illegally collect, process or use personal data. The civil liabilities relate to tortious acts. Since personal data involves a data subject's privacy, a data subject whose privacy is impinged upon may also claim damages against a government agency pursuant to the State Compensation Act and against a non-government agency pursuant to the Civil Code.

The PDPA has incorporated some provisions under Directive 95/46/EC. In addition, the MoJ has published some introductions on the OECD guidelines and the APEC Privacy Framework as references for various industries and data protection authorities to implement the PDPA.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the powers of the authority.

The MoJ is in charge of establishing the Enforcement Rules to the PDPA, which define and clarify, among others:

- terms under the PDPA;
- a data owner's obligations to supervise a commissioned agency;
- proper security measures;
- what constitutes a written consent and a proper notification; and
- how a data subject exercises rights.

The MoJ also answers questions from various government agencies and non-government agencies regarding how to interpret and comply with the PDPA. The MoJ's interpretations cannot bind the courts, but would usually be referred to and adopted by the courts in making judgments.

The enforcement of the PDPA is administered by the central and local (city and county) government authorities which supervise the business operations of non-government agencies. The central government authorities may impose restrictions on a non-government agency's cross-border transfers of personal data and designate certain non-government agencies to establish a plan to maintain the security of personal data files or how to dispose of those files after they cease business operations. In addition, the purposes of the collection, processing, and use and categories of personal data are designated jointly by the MoJ and the central government authorities.

Both the central and local government authorities have the power to carry out audits and inspections. To audit and inspect any non-compliance, they may access the premises of non-government agencies, require information, copy and retain documents and other objects, and impose rectification orders and administrative penalties on non-government agencies.

3 Breaches of data protection

Can breaches of data protection lead to criminal penalties? How would such breaches be handled?

The following breaches may lead to criminal penalties:

- the illegal collection, processing or use of personal data, causing injury to another (article 41 of the PDPA);
- failure to obey a central government authority's order imposing restrictions on cross-border transfers of personal data, causing injury to another (article 41 of the PDPA); and
- the illegal change or deletion of personal data files or employment of any other illegal means with an intent to make unlawful profit for oneself or a third party, or with an intent to damage the interest of another, thereby impeding the accuracy of personal data files and causing injury to another (article 42 of the PDPA).

Criminal offences can be prosecuted by an injured person or a public prosecutor upon an injured person's complaint. If the criminal offences under article 41 are committed with an intent to make profit or the criminal offences under article 42 are committed against a government agency, they can be prosecuted by a public prosecutor solely on his or her initiative.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The PDPA applies to all the public and private bodies who collect, process or use personal data. The following activities are exempt from the application of the PDPA:

- the collection, processing or use of personal data by an individual in the course of a personal or family activity; and
- the collection, processing or use of audio-visual information in a public place or a public activity, which is not associated with any other personal data.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The PDPA regulates the use of personal data for marketing purposes; it does not specifically deal with electronic marketing. Although electronic marketing is dealt with under the Guidelines Governing the Consumer Protection in E-Commerce promulgated by the Consumer Protection Committee, the legislature has not passed a law specifically regulating electronic marketing.

The interception of communications and the monitoring and surveillance of individuals are covered by the Communications Protection and Detection Act and the Criminal Code. Since an individual's communications and activities are personal data and involve privacy, the illegal interception of an individual's communications and the illegal monitoring and surveillance of an individual's activities also constitute breaches of the PDPA and are tortious acts under the Civil Code.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

The PDPA is the only legislation that specifically regulates personal data protection. There are many other laws and regulations that cover personal data. For example, the Act Governing the Freedom of Government Information regulates the disclosure by government agencies of government information that may contain personal data. The Financial Holding Company Act regulates sharing among a financial holding company's subsidiaries of their clients' basic and transaction information. The Pharmaceutical Affairs Act regulates the drug safety surveillance and reporting system that includes patients' personal data.

7 PII formats

What forms of PII are covered by the law?

The PDPA has extended its protection from personal data for computer-processing to all personal data regardless of whether they are in electronic records or manual files.

8 Extraterritoriality

Is the reach of the law limited to data owners and data processors established or operating in the jurisdiction?

Under the PDPA, data owners are referred to as government agencies and non-government agencies (private sector). The PDPA defines a 'non-government agency' broadly to include a natural person, a juristic person and an unincorporated association. Pursuant to the book *Personal Data Protection Act's Interpretation and Practice*, written by the officials of the MoJ, a non-government agency that is subject to the PDPA is limited to a Taiwanese national or an entity registered in Taiwan, such as a foreign company which has established a branch office in Taiwan. A non-government agency must comply with the PDPA when collecting, processing or using an individual's personal data within Taiwan or a Taiwanese national's personal data outside the territory of Taiwan.

In addition, the MoJ has issued a directive confirming that the collection, processing and use of an individual's personal data by a foreign national or entity within Taiwan is also subject to the PDPA, regardless of whether such foreign national or entity is registered in Taiwan.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide services to owners?

The PDPA requires that data owners comply with the requirements under the PDPA. The Enforcement Rules of the PDPA require that persons who collect, process and use personal data under the commission and on behalf of data owners (ie, commissioned agencies) comply with the requirements applicable to the data owners. A data owner must duly supervise the commissioned agency to ensure the latter's compliance and is liable to data subjects for the commissioned agency's or its own non-compliance.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent? Give details.

The PDPA sets out different grounds for the legitimate processing of personal data, depending on whether a data owner is a government agency or a non-government agency.

A government agency may process personal data if it is for specific purposes and:

- the processing is necessary for the performance of job duties provided by law;
- the data subject has given his or her written consent; or
- the processing will not be detrimental to the interests of the data subject.

A non-government agency may process personal data if it is for specific purposes and:
- the processing is specifically permitted by law;
- the processor and the data subject have entered into or are negotiating a contract;
- the data is already in the public domain due to disclosure by the data subject or in a legitimate manner;
- it is necessary for statistics-gathering or academic research by an academic research institution for the public interest, provided that any information sufficient to identify the data subject has been removed;
- the data subject has given his or her written consent;
- it is for the public interest; or
- the data has been collected from a source accessible to the collector unless the interest of the data subject takes priority over that of the collector or processor.

11 Legitimate processing – types of data

Does the law impose more stringent rules for specific types of data?

Article 6 of the PDPA sets out distinct grounds for the legitimate processing of sensitive data. Since the grounds are too limited to meet certain industries' needs, the Executive Yuan has suspended the enactment of article 6 and proposed a draft bill to amend article 6 to include other legal grounds. The draft bill is pending the legislature's reading.

Under the draft bill, sensitive data includes medical history, medical treatments, genealogy, sex life, health-check results and criminal records.

Before the draft bill is passed by the legislature and takes effect, the grounds for the legitimate processing of personal data apply to the processing of sensitive data.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose data they hold? What must the notice contain and when must it be provided?

If a data owner collects personal data directly from a data subject, the data owner must inform the data subject of the following information at the time of collection:
(i) the identity of the data owner;
(ii) the purposes for which his or her data is collected;
(iii) the type of data collected;
(iv) the term, place and method of use and the persons who may use the data;
(v) the data subject's rights (explained in question 14); and
(vi) the consequences of his or her failure to provide the required personal data (article 8 of the PDPA).

If a data owner collects personal data indirectly from a data subject, the data owner must inform the data subject of the data source and information (i) to (v) above no later than the first time they use such personal data to contact the data subject (article 9 of the PDPA).

13 Exemption from notification

When is notice not required (for example, where to give notice would be disproportionate or would undermine another public interest)?

The notification requirement under article 8 is exempt if:
(i) it is specifically permitted by law;
(ii) the collection is necessary for the performance of job duties provided by law or the fulfilment of legal obligations;
(iii) notification will affect a governmental agency's performance of its job duties;
(iv) notification will prejudice a third party's material interest; or
(v) the data subjects already have such information.

The notification requirement under article 9 is exempt if:
- any of the above exemption situations (i) to (v) exists;
- the data subject has disclosed such information by him or herself, or when the information has been publicised legally;
- the notification may not be made to the data subject or his legal representative;
- it is for the public interest and necessary for the purpose of statistics or academic research and the data has been processed to such an extent that the data subject cannot be identified; or
- the personal data is collected by the mass media for the purpose of news reporting in the public interest.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

A data subject has rights to access his or her data to check and review them, have a copy of the data, supplement or revise the data, demand the data owner to cease its collection, processing or use of the data, and demand the data owner to delete the data.

Unless the processing or use are necessary for the performance of job duties or fulfilment of legal obligations or the data subject has consented in writing to the processing or use, a data owner must cease the processing or use of personal data if the data subject disputes the accuracy of the data, and must delete or cease the processing or use of personal data if the purposes of processing or use no longer exist or the term of use expires.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

A data owner must ensure the accuracy of personal data and update or supplement personal data on its own initiative or upon the data subject's request.

If the failure to provide accurate personal data is attributed to a data owner, the data owner should notify the persons to whom the data was provided as soon as the data owner updates or supplements the data.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The PDPA does not impose a specific amount of data that can be held or a retention period. A data owner may retain personal data when the purposes of processing or use exists or during the term of use. After that, it may retain the personal data if it is necessary for the performance of job duties or the fulfilment of legal obligations or the data subject has consented in writing to the same. The retention is deemed to be necessary for a data owner's performance of job duties or fulfilment of legal obligations if:
- the retention period provided by law or contract has not expired;
- the deletion will be detrimental to the interests of the data subject; or
- there is any other legitimate ground for the retention.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

A data owner may use personal data only if it is for, and reasonably associated with, the specific and lawful purposes for which the personal data has been collected.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

A government agency may use personal data for a specific and lawful new purpose (other than those for which the personal data has been collected) if:

- such use is specifically permitted by law;
- it is to further national security or public interest;
- it is to prevent any injury or damage to human life, body, freedom or property;
- it is to prevent any third person's material right or interest from being prejudiced;
- it is necessary for statistic-gathering or academic research by an academic research institution for the public interest, provided that any information sufficient to identify the data subject has been removed;
- it may benefit the data subject; or
- the data subject has given written consent after the data owner has notified the data subject of the following information:
  - what the other purposes are;
  - the scope of use; and
  - how the data subject's rights and interests will be affected if he or she chooses not to give consent.

A non-government agency may use personal data for a specific and lawful new purpose (other than those for which the personal data has been collected) if the use meets the above criteria, except that the requirement that it benefits the data subject does not apply to a non-government agency.

Security obligations

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

The PDPA requires a data owner to have in place appropriate measures to prevent personal data or their files from being stolen, altered, damaged, destroyed, lost or disclosed.

The Enforcement Rules to the PDPA require a data owner to adopt, and to procure its commissioned agency to adopt, technical and organisational measures which are reasonable and sufficient to protect personal data. Such measures are recommended to include the following:

- allocation of personnel to enforce the measures and sufficient resources;
- identification of the scope of personal data;
- a personal data risk valuation and management mechanism;
- mechanisms for prevention, notification, and handling of accidents;
- internal management procedures for collection, processing, and use of personal data;
- security management and personnel management;
- education and training;
- IT infrastructure security management;
- data security auditing mechanisms;
- maintenance of access records, track log files and relevant evidence; and
- continuous improvement on security and maintenance measures.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

If personal data is stolen, leaked, or altered or the data subjects' interests may otherwise be compromised because of a data owner's failure to comply with the PDPA, the data owner must notify the data subjects of the incident and the remedies that the data owner has adopted as soon as the data owner has carried out an investigation of the incident.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The PDPA requires that a government agency which holds personal data files must assign personnel to administer the security and maintenance of those files, but does not specify the legal responsibilities of such personnel.

The PDPA does not impose the same obligation on a non-government agency.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Although the PDPA does not expressly require a data owner to maintain internal records or establish internal processes or documentation, the Enforcement Rules to the PDPA recommend that the security measures that a data owner must adopt include data security auditing mechanisms and maintenance of access records, track log files, and relevant evidence.

Registration and notification

23 Registration

Are owners and processors of PII required to register with the supervisory authority? Are there any exemptions?

The registration requirements under the CPDPA were abolished along with the president's promulgation of the PDPA on 26 May 2010.

24 Formalities

What are the formalities for registration?

Not applicable – see question 23.

25 Penalties

What are the penalties for a data owner or processor for failure to make or maintain an entry on the register?

Not applicable – see question 23.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable – see question 23.

27 Public access

Is the register publicly available? How can it be accessed?

Not applicable – see question 23.

28 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable – see question 23.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The PDPA simply provides that a commissioned agency's conduct will be deemed as the data owner's conduct. Hence, a data owner's transfer of personal data to its commissioned agency will be deemed the internal processing by the data owner of the personal data and subject to the restrictions stipulated for the processing thereof. See question 10.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

The disclosure of personal data to a third party constitutes the use of the personal data and thus is subject to the restrictions stipulated for the use thereof. See questions 17 and 18.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The central government authorities may impose restrictions on a non-government agency's cross-border transfers of personal data if:

- the transfer would prejudice any material national interest;
- it is prohibited or restricted under an international treaty or agreement;
- the country to which the personal data is to be transferred does not afford sound legal protection of personal data, thereby affecting the interests of the data subjects; or
- the purpose of the transfer is to evade restrictions under the PDPA.

On 25 September 2012, the National Communications Commission issued a blanket order prohibiting communications enterprises from transferring subscribers' personal data to mainland China on the grounds that the personal data protection laws in mainland China are still inadequate.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

No. The transfer of personal data outside Taiwan does not require the transferor to notify or seek the authorisation from a supervisory authority.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions on cross-border transfers apply equally to the transfers made to a commissioned agency or a third-party data owner. They do not apply to onward transfers.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

Individuals have the right to view a copy of their personal data. On request, a data owner must provide a copy thereof to the individual unless:

- it would be detrimental to national security, diplomatic or military secrets, economic interests as a whole, or any other material national interests;
- it would impede a government agency's performance of job duties; or
- it would be detrimental to the material interests of the data owner or a third party.

35 Other rights

Do individuals have other substantive rights?

Individuals also have the right to:

- access his or her data to check and review them;
- supplement or revise the data;
- demand the data owner to cease its collection, processing or use of the data; and
- demand the data owner to delete the data.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals are entitled to monetary damages based on the amount of their actual loss that they have suffered as a result of the breach of the PDPA by a data owner. They are also entitled to monetary compensation for distress if any of their intangible rights (eg, privacy and reputation) is damaged. The courts may set the amount of damages at NT$500 to NT$20,000 for each incident per person if an individual cannot prove the amount of actual damages or compensation.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

If a government agency rejects an individual's request relating to any of the rights described under questions 34 and 35, the individual may file an administrative appeal with a supervisory authority of the government agency and if the appeal is dismissed, file an administrative complaint with a High Administrative Court to enforce his or her right. If a non-government agency rejects such request, the individual may file a civil complaint with a district court to enforce his or her right.

Individuals must file a civil complaint with a district court to claim monetary damages or compensation described under question 36.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No.

Supervision

39 Judicial review

Can data owners appeal against orders of the supervisory authority to the courts?

A government agency may not appeal against orders of its supervisory authority. A non-government agency will receive orders from a data protection authority described in question 2 and may appeal against such orders to the data protection authority's supervisory authority.

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

See question 3.

41 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The PDPA does not contain specific rules regarding cookies or equivalent technology. To the extent the use of such technologies involves the collection, processing, or use of personal data, the requirements relating to the collection, processing, or use under the PDPA will apply.

Update and trends

The PDPA took effect on 1 October 2012. Since it applies to all public and private sectors, imposes new requirements, and enhances legal liabilities for non-compliance, the MoJ has been clarifying the inquiries from various industries. The clarification by the MoJ would be an important reference to the courts when they make judgments.

In addition, article 6 of the PDPA prohibits the collection, processing, and use of sensitive data, unless any exemption condition is met. Since the exemption conditions are too limited to meet certain industries' needs, the Executive Yuan has suspended the enactment of article 6 and proposed a draft bill to amend article 6 to include other exemption conditions. Once the draft bill passes the legislature's reading and becomes enacted, the collection, processing, and use of sensitive data will be subject to distinct and stricter exemption conditions.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

Sending marketing information by e-mail, fax or telephone to data subjects constitutes the use of their personal data. A non-government agency must comply with the requirements relating to the use of personal data described under questions 17 and 18 (eg, a data subject has consented in a contract or given a separate written consent) when it sends marketing information to data subjects (opt-in rules). A non-government agency must immediately cease the use of personal data for such marketing purposes if the data subject has notified the non-government agency that he or she does not wish to receive such marketing information (opt-out rules).

理律法律事務所
LEE AND LI
ATTORNEYS-AT-LAW

Ken-Ying Tseng **kenying@leeandli.com**
Rebecca Hsiao **rebeccahsiao@leeandli.com**

9F, 201 Tun Hua N Road
Taipei 10508
Taiwan

Tel: +886 2 2715 3300
Fax: +886 2 2713 3966
www.leeandli.com