Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Ninth edition
ISBN 978-1-83862-322-7

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

Data Protection & Privacy

2021

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the ninth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Canada and Romania.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY®
Getting The Deal Through

London
August 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Introduction 5
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

EU overview 9
Aaron P Simpson, Claire François and James Henderson
Hunton Andrews Kurth LLP

The Privacy Shield 12
Aaron P Simpson and Maeve Olney
Hunton Andrews Kurth LLP

Australia 17
Alex Hutchens, Jeremy Perier and Meena Muthuraman
McCullough Robertson

Austria 25
Rainer Knyrim
Knyrim Trieb Rechtsanwälte

Belgium 33
David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

Brazil 45
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra
Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados

Canada 53
Doug Tait and Catherine Hamilton
Thompson Dorfman Sweatman LLP

Chile 60
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
Magliona Abogados

China 67
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

Colombia 76
María Claudia Martínez and Daniela Huertas Vergara
DLA Piper

France 83
Benjamin May and Farah Bencheliha
Aramis Law Firm

Germany 95
Peter Huppertz
Hoffmann Liebs Fritsch & Partner

Greece 102
Vasiliki Christou
Vasiliki Christou, Attorney at Law

Hong Kong 109
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

Hungary 118
Endre Várady and Eszter Kata Tamás
VJT & Partners Law Firm

India 126
Stephen Mathias and Naqeeb Ahmed Kazia
Kochhar & Co

Indonesia 133
Abadi Abi Tisnadisastra, Prihandana Suko Prasetyo Adi and Noor Prayoga Mokoginta
AKSET Law

Italy 142
Paolo Balboni, Luca Bolognini, Antonio Landi and Davide Baldini
ICT Legal Consulting

Japan 150
Akemi Suzuki and Tomohiro Sekiguchi
Nagashima Ohno & Tsunematsu

Malaysia 159
Jillian Chia Yan Ping and Natalie Lim
SKRINE

Malta 166
Terence Cassar, Ian Gauci and Bernice Saliba
GTG Advocates

Mexico 174
Abraham Diaz and Gustavo A Alcocer
OLIVARES

Netherlands 182
Inge de Laat and Margie Breugem
Rutgers Posch Visée Endedijk NV

New Zealand 190
Derek Roth-Biester and Megan Pearce
Anderson Lloyd Lawyers

Portugal 197
Helena Tapp Barroso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Romania 206
Daniel Alexie, Cristina Crețu, Flavia Ștefura and Laura Dinu
MPR Partners | Maravela, Popescu & Asociații

Russia 214
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Vasilisa Strizh and Brian L Zimbler
Morgan Lewis

Serbia 222
Bogdan Ivanišević and Milica Basta
BDK Advokati

Singapore 229
Lim Chong Kin and Charis Seow
Drew & Napier LLC

South Korea 243
Young-Hee Jo, Seungmin Jasmine Jung and Kwangbok Kim
LAB Partners

Sweden 253
Henrik Nilsson
Wesslau Söderqvist Advokatbyrå

Switzerland 261
Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

Taiwan 271
Yulan Kuo, Jane Wang, Brian Hsiang-Yang Hsieh and Ruby Ming-Chuang Wang
Formosa Transnational Attorneys at Law

Turkey 278
Esin Çamlıbel, Beste Yıldızili Ergül and Naz Esen
Turunç

United Kingdom 286
Aaron P Simpson, James Henderson and Jonathan Wright
Hunton Andrews Kurth LLP

United States 296
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Taiwan

Yulan Kuo, Jane Wang, Brian Hsiang-Yang Hsieh and Ruby Ming-Chuang Wang
Formosa Transnational Attorneys at Law

LAW AND THE REGULATORY AUTHORITY

Legislative framework

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

Taiwan has a one-piece legislation, the Personal Data Protection Act (PDPA), which affords comprehensive protection with respect to the use, collection and processing of PII by governmental agencies and private entities. The PDPA sets forth statutory requirements that must be met by entities for the use, collection and processing of PII. Special protections are imposed upon an entity if the PII used, collected or processed by the entity falls into the category of 'sensitive data', which includes a person's health records, genetic information, sexual history and criminal history. An entity that violates the requirements imposed by the PDPA will be subject to provisions imposing both civil and criminal liability on the entity. The PDPA also gives an administrative agency having proper jurisdiction the authority to impose administrative penalties upon the entity.

The PDPA does not explicitly cite any foreign legislation. However, according to the historical record, the drafters of the PDPA did consider the provisions of Directive 95/46/EC, the OECD guidelines and the Asia-Pacific Economic Cooperation's privacy framework when drafting the PDPA.

Data protection authority

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

The PDPA does not give any single governmental agency overriding authority to oversee enforcement of the PDPA. As such, there is no particular governmental agency in Taiwan that has been actively policing personal data protection practices. The PDPA, however, requires Taiwan's Ministry of Justice (an equivalent to the US Department of Justice), to set forth guiding principles for all other governmental agencies, central and local, to take into account when enforcing the provisions of the PDPA.

Moreover, in response to the European Union's enforcement of General Data Protection Regulation (GDPR), Taiwan's National Development Council (NDC), a policy-advising agency affiliated to the Executive Yuan (the highest agency of the executive branch), established the Personal Data Protection Office (Office) on 4 July 2018. One of the main functions of the Office is to coordinate the enforcement of PDPA by different governmental agencies and to examine the current regulations of the PDPA. The Office was appointed by the Executive Yuan to monitor Taiwan's personal data protection issues and the enforcement of PDPA.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The PDPA does not give any particular governmental agency overriding authority to enforce the data protection law. However, the PDPA does require the Ministry of Justice to set forth guiding principles.

In response to the EU's enforcement of the GDPR, the Personal Data Protection Office was appointed by the Executive Yuan to monitor Taiwan's personal data protection issues and the enforcement of PDPA.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Any breach of the obligations imposed by the PDPA may result in liabilities, civil and criminal, as well as administrative penalties and orders.

An administrative agency having proper jurisdiction over a breach could impose upon the breaching entity a cease and desist order that compels the breaching entity to immediately cease collecting, processing and using the relevant PII. The agency could also order the breaching entity to delete the PII possessed by the breaching entity, or to confiscate or destroy the PII that the breaching entity unlawfully collected. The agency may also publish the facts of such a data breach and the name of the breaching entity and its representative.

Administrative penalties may be a fine imposed on the breaching entity and its representative of between NT$20,000 and NT$500,000.

A natural person responsible for the breach will also face criminal penalties, including imprisonment for up to five years and a fine of up to NT$1 million.

SCOPE

Exempt sectors and institutions

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

The Personal Data Protection Act (PDPA) is applicable to all sectors and organisations, private and public, and all kinds of activity. At the same time, however, some other individual statutes impose specific data protection for some particular types of personally identifiable information (PII). For instance, financial institutions operate under stringent obligations to maintain the confidentiality of their clients' financial data. Labour laws also impose on employers' certain obligations to keep their employees' personal data confidential.

Communications, marketing and surveillance laws

6 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 does not specifically address invasions of privacy via interception of communications, electronic marketing or monitoring, and conducting surveillance on individuals. Nevertheless, if the invasion of privacy concerns PII as defined in the PDPA, the PDPA will certainly regulate that activity. Additionally, anyone conducting illegal surveillance will be in violation of Taiwan's Criminal Code or the Communication Security and Surveillance Act. These statutes make unlawful surveillance a crime and impose upon offenders' criminal penalties, including imprisonment, detention and fines.

Other laws

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

There are many other laws and regulations specifically applied to various activities and industries that provide specific data protection to individuals. For example, the Human Biobank Management Act mandates special protection for the PII of participants who provide biological specimens. The Enforcement Rules for the Financial Technology Development and Innovative Experimentation Act (Sandbox Act) provide specific rules to manage and protect PII collected from those participating in experiments. Also, the Employment Service Act stipulates that employers are not allowed to force employees or job seekers to provide unnecessary personal information.

PII formats

8 What forms of PII are covered by the law?

The PDPA covers all PII without limitation to specific formats of personal data.

Extraterritoriality

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

No. Even if the use, collection or processing occurs outside the territory of Taiwan, the PDPA is applicable if the data subject is a Taiwan citizen.

The PDPA explicitly provides that a Taiwan entity or individual will be subject to the obligations set forth by the PDPA for their use, collection or processing of PII of other Taiwan citizens outside the territory of Taiwan.

Covered uses of PII

10 Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

Yes, the PDPA covers all processing and use of PII. The PDPA does not distinguish between those who control or own PII and does not impose different duties and obligations.

The definitions of PII collection, processing and use under the PDPA are as follows:

- collection: to collect PII in any form or in any way;
- processing: to record, input, store, compile, correct, duplicate, retrieve, delete, output, connect or internally transmit PII for the purpose of establishing or using a PII file; and
- use: to use PII in any way other than processing.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 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?

According to the Personal Data Protection Act (PDPA), a non-governmental entity (including natural persons and private agencies) may collect and process personally identifiable information (PII) for a specific purpose in the following situations:

- the collection or processing of PII is permitted by law;
- the collecting or processing party and the PII subject (individual) form or are going to form a contractual relationship, and the collection and processing of PII is done with proper safety measures;
- the PII is published by the PII subject or is legally published by a third person;
- the collection or processing of the PII is done by a research entity where the collection or processing is necessary to perform statistical or academic research in the public interest and the collecting party or the providing party of such PII has altered the PII such that the subject cannot be identified by the PII;
- the collection or processing is made with the PII subject's consent;
- the collection or processing of the PII is done to enhance the public interest;
- the PII is collected from publicly available resources; and
- the right or interest of the PII subject will not be harmed.

However, where the PII is collected from publicly available resources, the PII shall not be further collected or processed if the data subject objects to such collection.

Also, according to the PDPA, use of the PII will be permitted if such use is within the specific purpose for collecting and processing the PII.

Moreover, while requesting the PII subject's consent, the collecting party must disclose the following information:

- the name of the authority collecting the PII;
- the purpose of collection;
- the category of the PII;
- the period, area, object and method of use of the PII;
- the rights of the data subject to request:
  - a review of his or her PII;
  - to make duplications of his or her PII;
  - to supplement or correct his or her PII;
  - to have the collection, processing or use of his or her PII discontinued; and
  - to have his or her PII deleted from the record; and
  - to exercise his or her rights if he or she chooses not to agree to the collection.

However, in the following situations, the above disclosures are not required:

- the exemption from the obligation to disclose is permitted by law;
- the collection of PII is necessary for a governmental agency to perform its official duties or for a non-government entity to fulfil a legal obligation;
- the disclosure will impede a governmental agency in performing its official duties;
- the disclosure will impair the public interest;
- the PII subject should have already known the content of the notification; and
- the collection of personal information is for non-profit purposes, and it clearly will not harm the interest of the data subject.

Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

The PDPA does impose more stringent rules for specific types of PII. Sensitive PII, such as medical records, medical treatment, genetic information, sexual history, health examinations and criminal records can be collected, processed and used only in the following situations:

- the collection, processing and use of PII is permitted by law;
- the collection, processing and use of PII is necessary for a governmental agency to perform its official duties or for a non-government entity to fulfil a legal obligation, and proper safety measures are taken during and after the collection, processing and use of PII;
- the PII is published by the PII subject (individual) or is legally published by a third person;
- 1 the collection, processing or use of PII is made by a governmental or research entity for the purpose of enhancing medical treatment or health or to prevent criminal activities, where the collection, processing and use of PII is necessary to perform statistical or academic research, and where the collecting party or the providing party of such PII has altered the PII such that the individual cannot be identified;
- the collection, processing and use of PII is done to assist a governmental or non-governmental entity in performing official duties or fulfilling a legal obligation, and proper safety measures are taken during and after the collection, processing and use of PII; and
- to the extent permitted by law, the collection, processing and use of PII is made with the PII subject's written consent.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

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

Yes, in accordance with the Personal Data Protection Act (PDPA), if the personally identifiable information (PII) is collected without the consent of the data subject, the PII owner is required to notify the data subject of its possession of his or her PII before the owner processes or uses the PII. The notice must include the following information:

- the source of collection;
- the name of the authority collecting, processing or using the PII;
- the purpose of the collection;
- the category of the PII;
- the period, area, object and method of use of the PII; and
- the rights of the data subject to request a review of his or her PII, to make duplications of his or her PII, to supplement or correct his or her PII, to have the collection, processing or use of his or her PII discontinued, and to have his or her PII deleted from the record.

Exemption from notification

14 | When is notice not required?

In the following situations, notice to the data subject of the use and processing is not required:

- the exemption from the obligation to give notification is permitted by law;
- the collection of the PII is necessary for a governmental agency to perform its official duties or for a non-governmental entity to fulfil a legal obligation;
- giving notice will impede a governmental agency in performing its official duties;
- giving notice will impair the public interest;
- the PII subject should have already known the content of the notification;
- the collection of personal information is for non-profit purposes, and the collection will clearly not harm the interest of the data subject;
- the PII is published by the data subject or is legally published by a third person;
- the PII owner cannot inform the data subject or his or her representative;
- the processing or use of the PII is done by a research entity where it is necessary to perform statistical or academic research in the public interest and the collecting party or the providing party of such PII has altered the PII such that the individual cannot be identified; and
- the PII is collected by the mass media for the purpose of reporting news in the public interest.

Control of use

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

The PDPA affords data subjects the right to request the PII owner to allow a review of his or her PII, to provide duplications of his or her PII, to supplement or correct his or her PII, to cease collecting, processing or using his or her PII, and to have his or her PII deleted from the record.

Data accuracy

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

The PDPA does not set forth standards for the quality, currency and accuracy of PII. However, the PDPA requires the PII owner to maintain the accuracy of PII and to actively supplement or correct the PII, or to do so upon request by the data subject. Additionally, if the accuracy of the PII is in dispute, the PII owner must actively cease processing or using the PII or do so upon request by the data subject. However, if the processing or use of the PII is necessary to perform official duties or to fulfil legal obligations, or is consented to by the data subject, the PII owner may continue its processing or use of the PII after recording that the PII is in dispute.

Amount and duration of data holding

17 | 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 restrict the amount of PII that may be held or the specific length of time it may be held. Nevertheless, the PDPA requires the PII owner to cease processing or using the PII once the specific purpose of the collection, processing or use of the PII no longer exists or the term of such purpose has expired. However, if processing or using the PII is necessary to perform official duties or to fulfil legal obligations, or is consented to by the data subject, the PII owner may continue to process or use the PII.

Finality principle

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

Yes, the purposes for which PII can be used are restricted by the PDPA. The PDPA provides a 'finality principle' under which the rights and interests of data subjects must be respected while the PII owner collects, processes or uses PII, and any collection, processing or use of PII must be conducted in good faith, must not go beyond specific purposes and must be performed in connection with the purpose of the collection.

Use for new purposes

19 | 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?

Yes, there are some exceptions from the finality principle. The PDPA allows PII to be used for new purposes if any one of the following situations exists:

- using PII for a new purpose is permitted by law;
- using PII for a new purpose is done to enhance a public interest;
- using PII for a new purpose is to prevent harm to the life, body, freedom or property of the data subject (individual);
- using PII for a new purpose is to prevent harm to the rights and interests of other people;
- PII is used by a research entity or governmental agency where using the PII for a new purpose is necessary to perform statistical or academic research to advance the public interest, and the collecting party or the providing party of such PII has altered the PII so that the individual cannot be identified;
- using PII for a new purpose is agreed to by the data subject; and
- using PII for a new purpose will benefit the rights of the data subject.

However, none of these exemptions applies to any sensitive data.

SECURITY

Security obligations

20 | What security obligations are imposed on PII owners and service providers that process PII on their behalf?

A governmental agency or non-governmental entity keeping possession of any personally identifiable information (PII) must adopt appropriate cybersecurity measures to prevent the PII from being stolen, altered, damaged, destroyed or disclosed. If the PII owner is a governmental agency, it is required to assign specific persons to be in charge of the security of PII. Also, the Personal Data Protection Act (PDPA) Enforcement Rules provide guidelines for such security measures. For example, the PII owner may assign and allocate personnel to manage PII, establish a mechanism to evaluate risk, to prevent leaks, to deal with any accidental incidents, establish internal rules, hold educational training and maintain the security system for regular periods. Moreover, the central government may require non-governmental entities to stipulate internal principles to protect the safety of PII, including how PII will be disposed of after the termination of the relevant business.

Notification of data breach

21 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The PDPA requires PII owners to notify data subjects of any data breaches if a breach results in PII being stolen, altered, damaged, destroyed or disclosed. In addition, some relevant PII regulations specifically applied to particular industries also require PII owners to report data breaches to the relevant governmental authorities. For example, PII owners in the banking and insurance industries are required by the regulations made by the Financial Supervisory Commission to report data breaches to the Commission.

INTERNAL CONTROLS

Data protection officer

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

In accordance with the Personal Data Protection Act (PDPA), a governmental agency keeping possession of PII is required to appoint a data protection officer (DPO), but this does not apply to a non-governmental entity. The responsibility of the DPO is to prevent personally identifiable information (PII) from being stolen, altered, damaged, destroyed or disclosed. However, the guidelines for security measures afforded by the PDPA Enforcement Rules suggest that a non-governmental entity appoint a DPO to manage the PII that it possesses. In addition, some relevant PII regulations specifically applied to particular industries also require PII owners to appoint a DPO. For example, the regulations applicable to banks, insurance providers and short-term educational centres require entities in these industries to appoint a DPO.

Record keeping

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

The PDPA does not require PII owners or processors to maintain internal records of their processing or use of PII. However, the PDPA Enforcement Rules suggest that PII owners or processors, whether governmental or non-governmental entities, keep internal records to protect the security of PII. On the other hand, some relevant PII regulations specifically applicable to particular industries require PII owners or processors to maintain internal records of the use of PII. For example, the regulations made by the Financial Supervisory Commission require PII owners in the banking and insurance industries to maintain such internal records.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

The PDPA does not address approaches for privacy-by-design or risk assessments for privacy impacts. However, the PDPA Enforcement Rules suggest that PII owners or processors, whether governmental or non-governmental entities, establish a mechanism to evaluate the risk of collecting, processing and using PII. Some relevant PII regulations specifically applied to particular industries, however, require PII owners or processors to periodically make risk assessments on their collecting, processing or use of PII. For example, online shops and platforms, banks and insurance providers, real estate agencies and short-term educational centres are obligated to make such PII risk assessments.

REGISTRATION AND NOTIFICATION

Registration

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

Personally identifiable information (PII) owners or processors are not required to register with the supervising authority before carrying out the collection, processing or use of PII.

Formalities

26 | What are the formalities for registration?

Not applicable.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

Refusal of registration

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

Not applicable.

Public access

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

Not applicable.

Effect of registration

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

Not applicable.

Other transparency duties

31 | Are there any other public transparency duties?

In accordance with the Personal Data Protection Act (PDPA), a governmental agency is required to publish the following information on the internet or by other proper means for review:

- the name of a PII file;
- the name of the governmental entity keeping the PII file and its contact information;
- the legal basis for and purpose of keeping the PII; and
- the classification of PII.

Non-governmental entities keeping PII are not obligated to make such publication.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

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

There is no provision of the Personal Data Protection Act (PDPA) specifically regulating the transfer of personally identifiable information (PII) to entities that provide outsourced processing services. However, because the transfer of PII is categorised as an activity of processing or using PII under the PDPA, the transfer of PII to entities that provide outsourced processing services must comply with all provisions regulating the processing or use of PII. As such, while transferring PII to another entity, the PII owner is obligated to prevent the PII from being stolen, altered, damaged, destroyed or disclosed.

Restrictions on disclosure

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

Disclosing PII to other recipients must be done in accordance with the regulations for the use of PII under the PDPA. That is, for a non-governmental entity, if disclosing PII to other recipients is within the scope of a specific purpose for collecting and processing the PII, the PII owner may freely make such disclosure. Otherwise, the disclosure can be made only if it satisfies the requirements under which the use of PII for new purposes is allowed. However, the recipient must notify the data subject of its possession of PII before processing or using the PII. For the requirements of using PII for new purposes and contents of notification given by the recipients and their exceptions.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

The PDPA does not impose restrictions on international transfers of PII by governmental entities, but non-governmental entities are restricted by central government from transferring PII outside the jurisdiction if any one of the following situations occurs:

- the transfer involves significant national interests, such as national security, diplomatic or military secrets;
- a national treaty or agreement specifies other requirements on transfers;
- the country where the PII will be received lacks proper regulations on the protection of PII and the transfer might harm the rights and interests of data subjects; or
- the international transfer of PII is made to evade the provisions of the PDPA.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No, the PDPA does not require notification to or authorisation from a supervisory authority before or after engaging in a cross-border transfer of PII. However, because the central government may restrict non-governmental entities from transferring PII to other jurisdictions, as provided by the PDPA, it is prudent to confirm the legality with the supervisory authority before making any international transfer of PII.

Further transfer

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

The restriction on cross-border transfers applies to all non-governmental entities without differentiation between service providers or PII owners.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Yes, the Personal Data Protection Act (PDPA) gives data subjects the right to access their personal information held by personally identifiable information (PII) owners. Data subjects may request PII owners to allow a review of their PII or to provide duplications of their PII. However, under any one of the following situations, the above requests may be declined:

- the request might interfere with or harm national security, diplomatic or military secrets, economic interests, or other significant national interests;
- the request might interfere with the performance of official duties; or
- the request might negatively affect the interests of the PII owner or a third person.

Other rights

38 | Do individuals have other substantive rights?

In addition to the data subject's right to request PII owners to allow a review of his or her PII or to provide duplications of his or her PII, the PDPA provides data subjects with the right to have his or her data corrected, to cease the collection, processing or use of his or her PII, and to delete his or her PII. These rights of data subjects cannot be waived by data subjects.

Compensation

39 | 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?

Yes. Data subjects are entitled to monetary damages if their PII is breached. Below are the details:

- Compensation is not limited to loss of costs, as non-pecuniary damages such as emotional distress and loss of reputation are available. If the reputation of the PII subject is harmed due to the PII owner's breach of the PDPA, the PII subject may request the court to order the PII owner to restore his or her reputation.
- If the data subject has difficulty establishing the actual damages caused by the breach, he or she may request the court to grant compensation of an amount of no less than NT$500 but no more than NT$20,000 for each breach.
- If the breach causes damages to multiple data subjects by the same cause and fact, those victims are entitled to monetary compensation of no more than NT$200 million. However, if the value of the interests the breaching party may gain from the alleged violation is higher than NT$200 million, the victims are entitled to monetary compensation of no more than the established value of said interests.
- If the damages to multiple data subjects by the same cause and fact exceed NT$200 million, the limitation on compensation granted of the amount of no less than NT$500, as provided under the condition specified in the second bullet point above, shall not apply.
- Statute of limitation: the right to claim compensation will be blocked after two years from the date on which the data subject became aware of the damages and of the person(s) who is liable for the damages, or five years from the date of the occurrence of the damage.

If the breaching entity is a non-governmental entity, the entity may be free from liability if the entity successfully shows that the breach occurred without intent or negligence.

Enforcement

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

Data subjects seeking monetary damages or compensation must do so by filing a lawsuit at a court with proper jurisdiction.

Data subjects seeking remedies other than monetary damages or compensation where the PII owner is a non-governmental entity may go to the courts or report the matter to a governmental agency having proper jurisdiction.

If the PII owner is a governmental agency, data subjects must file an administrative appeal against said governmental agency and, if not successful, then file an administrative lawsuit.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

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

The Personal Data Protection Act will not apply where the collection, processing and use of personally identifiable information by a person is merely for personal and family activity, as well as where audio-visual information is collected, processed or used in public places or in public activities without association to other personal information (such as video recorded by dashboard cameras).

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Yes, if the personally identifiable information (PII) owner believes an order of a supervisory authority is in error, it may first appeal the order to its superior authority and then, if not successful, to the administrative court. However, for orders made by a supervisory authority mandating that the PII be detained or duplicated, the PII owner may directly file an objection to the supervisory authority at the time these orders are issued.

SPECIFIC DATA PROCESSING

Internet use

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

The Personal Data Protection Act (PDPA) does not contain specific provisions to regulate the use of cookies. However, if the information collected through cookies matches the definition of personally identifiable information (PII), the PDPA shall apply. Taking distributing targeted advertisements, for example, when the server collects PII from an individual, it must comply with the rules regulating PII collection under the PDPA; when the server analyses the PII collected, it must comply with the rules regulating PII processing and use under the PDPA; when the server uses its analysing report to distribute targeted advertisements, it must comply with the rules regulating PII use under the PDPA. In this regard, more and more websites utilise a pop-up window seeking users' consent to the collection, processing and use of their PII when the user visits the website for the first time.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

In accordance with the PDPA, when a non-governmental entity uses the PII collected to do marketing, regardless of whether it's via email, fax or telephone, it must stop if the data subject so requires. Also, when PII is first used by a non-governmental entity for marketing, the data subject must be advised of the measures for declining such marketing use. The expense for carrying out these measures must be borne by that entity.

Cloud services

45 Describe any rules or regulator guidance on the use of cloud computing services.

There are no specific rules or regulatory guidance on the use of cloud computing services. The use of cloud computing services must comply with all rules regulating the collection, processing and use of PII under the PDPA. Cloud services might trigger the following two issues under the PDPA:

- A cloud service provider and its corporate client maintain a contractual relationship between each other. As such, in accordance with the PDPA, the corporate client will be responsible for the cloud service provider's violation of the PDPA. Also, the corporate client is required to supervise the works of the cloud service provider with reasonable efforts, such as establishing a limited scope, classification, specific purpose of and time period for collecting, processing or using personal information, and keeping records of the works engaged in by the cloud service provider. The cloud service provider, on the other hand, must notify the corporate client if it believes that the client's instructions violate the PDPA.
- Cloud services often involve cross-border data transmissions.

UPDATE AND TRENDS

Key developments of the past year

46 Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The European Union's General Data Protection Regulation (GDPR), effective since 25 May 2018, has made a great impact upon many Taiwanese entities doing business with EU residents and entities. In response, Taiwan's National Development Council (NDC), a policy-advising agency affiliated to the Executive Yuan (the highest agency of the executive branch), established the Personal Data Protection Office (Office) on 4 July 2018. According to the NDC, the main functions of this Office include to consult with the European Commission (EC) for obtaining its recognition for adequate level of protection as set out in article 45 of the GDPR, and to be a platform coordinating the enforcement of the Personal Data Protection Act (PDPA) by different governmental agencies and to examine the current regulations of the PDPA. The Office was appointed by the Executive Yuan to monitor Taiwan's personal data protection issues and the enforcement of the PDPA.

To receive adequacy recognition from the European Commission, the Office completed the national evaluation report at the end of 2018. This report was thereafter filed to the European Commission's Directorate-General for Justice and Consumers (DG JUST). In early March 2019, the head of DG JUST, Tiina Astola, expressed European Commission's gratitude to Taiwan for its effort of working together with European Union to improve personal data protection policy. Although the report is still under review by the European Commission, the NDC announced that it would keep discussing this issue with the European Commission and adjust the PDPA if needed based on its continued communications with the European Commission and development of domestic industries. As of this writing, the Office has finished its first run of discussions with the European Commission. The European Commission's reviewing process is ongoing; the Office will work closely with the European Commission to adjust Taiwan's PDPA and the related regulations, if necessary.

萬國法律事務所
SINCE 1974 Formosa Transnational Attorneys at Law

Yulan Kuo
yulan.kuo@taiwanlaw.com

Jane Wang
jane.wang@taiwanlaw.com

Brian, Hsiang-Yang Hsieh
brian.hsieh@taiwanlaw.com

Ruby, Ming-Chuang Wang
ruby.wang@taiwanlaw.com

13F Lotus Building
136 Jen Ai Road
Section 3
Taipei 10657
Taiwan
Tel: +886 2 2755 7366
Fax: +886 2 2708 8435
www.taiwanlaw.com

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-322-7