ICLG

The International Comparative Legal Guide to:

Data Protection 2015

2nd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

A.G. Erotocritou LLC
Adsuar Muñiz Goyco Seda & Pérez-Ochoa, P.S.C.
Affärsadvokaterna i Sverige AB
Brinkhof
Cuatrecasas, Gonçalves Pereira
Dittmar & Indrenius
ECIJA ABOGADOS
ELIG, Attorneys-at-Law
Eversheds
Gilbert + Tobin
Gorodissky & Partners
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams LLP
Juridicon Law Firm
Jurisconsul
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Opice Blum, Bruno, Abrusio
& Vainzof Advogados Associados
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Portolano Cavallo Studio Legale
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

GLG
Global Legal Group

GLG
Global Legal Group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Head of Business Development
Dror Levy

Sales Director
Florjan Osmani

Commercial Director
Antony Dine

Account Directors
Oliver Smith, Rory Smith

Senior Account Manager
Maria Lopez

Sales Support Manager
Toni Hayward

Sub Editor
Amy Hirst

Senior Editor
Suzie Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
May 2015

ISBN
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

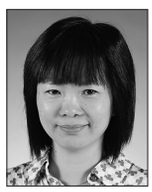
General Chapter:

Country Question and Answer Chapters:

Chapter 30

Taiwan


Ken-Ying Tseng


Rebecca Hsiao

Lee and Li, Attorneys-at-Law

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Personal Data Protection Act (PDPA) is a general law regulating the collection, processing and use of personal data. The PDPA was named the Computer-processed Personal Data Protection Act, which regulated all government agencies and certain entities in the private sector. The PDPA took effect on 1 October 2012 and applies to any person who collects, processes or uses personal data. The PDPA incorporates some provisions under Directive 95/46/EC. In addition, the Ministry of Justice (MoJ) has promulgated the Enforcement Rules to the PDPA and published some introductions in the OECD guidelines and the APEC Privacy Framework as references for various industries and data protection authorities to implement the PDPA.

1.2 Is there any other general legislation that impacts data protection?

If privacy is involved, the general protection of privacy as set forth under the Civil Code would be applicable. If a breach of confidentiality obligation is involved, the criminal sanctions as set forth in the Criminal Code may be incurred.

1.3 Is there any sector specific legislation that impacts 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.

1.4 What is the relevant data protection regulatory authority(ies)?

The MoJ is in charge of establishing the Enforcement Rules to the PDPA. 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. Both the central and local government authorities have the power to carry out audits and inspections and impose rectification orders and administrative penalties on non-government agencies.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  The PDPA defines "personal data" as a natural person's name, date of birth, national unified ID card number, passport number, special features, fingerprint, marital status, family background, educational background, occupation, contact information, financial status, social activities, sensitive data (defined below) and any other information that may be used to directly or indirectly identify a natural person.

- **"Sensitive Personal Data"**

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

- **"Processing"**

  The PDPA governs the collection, processing, and use of personal data. "Processing" means recording, inputting, storing, editing, correcting, duplicating, indexing, deleting, outputting, linking or internal transmission of personal data for the purpose of setting up or utilising a personal data file.

- **"Data Controller"**

  Under the PDPA, data controllers are referred to as government agencies and non-government agencies (private sector) that process, and/or use personal data. The PDPA defines a "non-government agency" broadly to include a natural person, a juristic person and an unincorporated association.

- **"Data Processor"**

  Under the PDPA, data processors are referred to as commissioned agencies that collect, process, and/or use personal data under the commission and on behalf of data controllers/owners.

- **"Data Owner"**

  Like data controllers, under the PDPA, data owners are referred to as government agencies and non-government agencies that collect, process, and/or use personal data.

- **"Data Subject"**

  A "data subject" is a natural person whose personal data is collected, processed, or used.

- **"Pseudonymous Data"**

  This is not applicable.

- **"Direct Personal Data"**

  This is not applicable.

- **"Indirect Personal Data"**

  Under the PDPA, information that may be used to indirectly identify a natural person indirectly means any information which alone is not sufficient for a data owner to identify a natural person, but when compared to or used together or in combination with other information, would be sufficient to identify a natural person.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  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; 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).

- **Lawful basis for processing**

  For personal data to be processed lawfully, a data owner must have a legal basis for each processing activity. The legal bases that may be relied upon by a government agency are: (i) processing that is necessary for the performance of job duties provided by law; (ii) written consent of the data subject; and (iii) processing that will not be detrimental to the interests of the data subject. The legal bases that may be relied upon by a non-government agency are: (i) processing that is specifically permitted by law; (ii) a contract that the non-government agency and the data subject have entered into or are negotiating; (iii) processing of the data that is already in the public domain due to disclosure by the data subject or in a legitimate manner; (iv) processing that 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; (v) written consent of the data subject; (vi) processing that is for the public interest; and (vii) processing of the data that 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.

  Article 6 of the PDPA sets out distinct legal bases for the lawful processing of sensitive data. Since the legal bases 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 bases. The draft bill is pending the legislature's reading. Before the draft bill is passed by the legislature and takes effect, the legal bases for the lawful processing of personal data apply to the processing of sensitive data.

- **Purpose limitation**

  Personal data may be collected or processed only for one or more specified and lawful purposes, and may be further used only if it is for, and reasonably associated with, the specific and lawful purpose(s) for which the personal data has been collected. A data owner may not use personal data for any new purpose unless the data owner may rely on a legal basis for the new purpose.

- **Data minimisation**

  Article 5 of the PDPA requires that the collection, processing, and use of personal data should not go beyond the specified purpose(s) and should be reasonable and fair. Thus, a data owner may process collect, process, and/or use only the personal data that is necessary for the relevant purpose.

- **Proportionality**

  Under Article 5 of the PDPA, the personal data that a data owner collects, processes, and/or uses should be proportionate to the relevant purpose.

- **Retention**

  A data owner may retain personal data when the relevant purpose 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: (i) the retention period provided by law or contract has not expired; (ii) the deletion will be detrimental to the interests of the data subject; or (iii) there is any other legal basis for the retention.

- *Other key principles*

  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.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  A data subject has the right to access his or her data to check and review them and have a copy of the data.

- **Correction and deletion**

  A data subject has the right to supplement or revise his or her data and demand the data owner to delete the data. A data owner 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.

- **Objection to processing**

  A data subject has the right to demand the data owner to cease its collection, processing or use of 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.

- **Objection to marketing**

  A data subject may notify a data owner at any time that he or she does not wish to receive the marketing information, and the data owner must immediately cease the use of the personal data for such marketing purpose.

- **Complaint to relevant data protection authority(ies)**

  If a government agency rejects a data subject's request relating to any of the rights described above, the data subject 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 data subject may file a civil complaint with a district court to enforce his or her right.

  A data subject may file a complaint with relevant central and/or local government authorities against any non-government agency for any violation of the PDPA.

- *Other key rights*

  Data subjects whose rights were damaged for the same cause may take a class action for damages.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

The registration requirements under the PDPA were abolished on 26 May 2010.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

This is not applicable.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

This is not applicable.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

This is not applicable.

5.5 What are the sanctions for failure to register/notify where required?

This is not applicable.

5.6 What is the fee per registration (if applicable)?

This is not applicable.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

This is not applicable.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

This is not applicable.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

It is not a mandatory requirement to appoint a Data Protection Officer. The Enforcement Rules to the PDPA simply suggest that personnel should be allocated for managing data protection matters.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

Although voluntarily appointing a Data Protection Officer does not provide a statutory exemption from any requirement under the PDPA, it may help to strictly implement a privacy compliance programme and therefore may reduce or avoid penalties or compensation liabilities in enforcement proceedings.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

The PDPA does not specify any qualifications for the Data Protection Officer.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

The PDPA does not specify the responsibilities of the Data Protection Officer.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, e-mail, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

Sending marketing information by post, telephone, email, or SMS text message to data subjects constitutes the use of their personal data. A data owner must rely on a legal basis relating to the use of personal data (e.g., the use is compatible with the original purpose(s) or the data subject has given a separate written consent for this new purpose) when it sends marketing information to data subjects (opt-in rules). A data owner 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).

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The MoJ has issued several rulings on marketing restrictions under a contractual relationship. The MoJ takes a narrow view i.e., that the products or services that a non-government agency promotes to customers based on their contractual relationship should be reasonably related to their contracts. It does not believe that it would be appropriate to provide marketing materials about third parties' products and services. Although the MoJ is active in educating non-government agencies on marketing restrictions, it is not responsible for enforcing the PDPA in respect of any violation thereof.

The Financial Supervisory Commission (FSC) has also issued several marketing guidelines for financial institutions to follow. Although the FSC is active in enforcing the PDPA, most sanctions that it imposes are related to illegal disclosures of personal data rather than breaches of marketing restrictions.

7.3 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Sending marketing communications in breach of any applicable restriction constitutes an illegal use of personal data which carries an administrative fine of up to NT$500,000 per breach. Other civil and criminal liabilities may be incurred as described under question 14.1 below.

7.4 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

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

7.5 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

This is not applicable.

7.6 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, they have not.

7.7 What are the maximum penalties for breaches of applicable cookie restrictions?

If the use of cookies involves illegal collection, processing, or use of personal data, the penalties described under question 14.1 below will apply.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

The central government authorities may impose restrictions on a non-government agency's transfer of personal data abroad if: (i) the transfer would prejudice any material national interest; (ii) it is prohibited or restricted under an international treaty or agreement; (iii) 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 (iv) the purpose of the transfer is to evade restrictions under the PDPA.

On 25 September 2012, the National Communications Commission (NCC) 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.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Companies will check whether (i) they have fulfilled their notification obligations to data subjects, (ii) they have a legal basis for the transfer (internal processing or disclosure to third parties), and (iii) the transfer is compatible with the specified purpose(s). If the transfer involves the processing of personal data by a commissioned agency, the companies will establish an audit mechanism to ensure the commissioned agency's compliance of all the requirements applicable to the companies under the PDPA.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

In principle, transfers of personal data abroad do not require any registration/notification or prior approval from a supervisory authority.

However, if a financial institution's cross-border transfer of personal data is to outsource any third party (whether an affiliate or a third-party vendor) to perform certain tasks offshore on its behalf, and such tasks relate to (i) the operation of the financial institution's registered business items as stated in its business licence, and/or (ii) the customers' information, the outsourcing requires the prior approval of the FSC.

To the extent that the prior approval described in question 5.8 above is required, a financial institution must file an application form along with all the required documents with the FSC. The filing package (in draft form) will be reviewed by the FSC. It will take about two to four weeks for the FSC to complete the review. Thereafter, the financial institution will have to submit a formal application. It will take the FSC about 60 days to grant its approval after the FSC receives the formal application.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

There is no specific law or guidance on whistle-blower hotlines regarding personal data protection.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

As there is no specific law or guidance on whistle-blower hotlines, anonymous reporting is not strictly prohibited or strongly discouraged.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

Hotlines do not require separate registration/notification or prior approval from data protection authorities.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Use of CCTV does not require separate registration/notification or prior approval from data protection authorities.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring practices are permitted if (i) the employees no longer have a reasonable expectation of privacy, and (ii) such monitoring is not expressly prohibited by law. Employees are deemed to not have a reasonable expectation of privacy if their employer has expressly announced the monitoring policy and/or employees have consented to the monitoring. Employees are deemed to have given an implied consent if they continue to use the equipment provided by the employer after the employer has announced the monitoring policy.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers may choose to issue a notice or obtain consent. Typically, employers will expressly announce the monitoring policy by sending e-mails and/or a written notice to each employee and publish the monitoring policy at the workplace.

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Only to the extent required under any employment or collective agreement.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Employee monitoring does not require any separate registration/notification or prior approval from data protection authorities.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The PDPA does not contain specific rules regarding processing of personal data in the cloud. Processing personal data in the cloud is permitted so long as it complies with the general requirements relating to the processing of personal data under the PDPA.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

A processor providing cloud-based services will be deemed a commissioned agency under the PDPA. A commissioned agency must comply with the requirements applicable to the data owner when the commissioned agency collects, processes, and uses personal data under the commission and on behalf of the data owner. In addition, a commissioned agency may collect, process, or use personal data only within the scope of the data owner's authorisation, and must notify the data owner immediately if the data owner's instructions violate the PDPA or any other laws or regulations.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Big data and analytics are permitted. There are no specific rules or guidance regarding the processing of personal data in the context of big data under the PDPA. 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. If data are anonymous, the PDPA does not apply.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

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, as promulgated by the MoJ, provide certain technical and organisational measures that a data owner may consider adopting based on the principle of proportionality, i.e., based on the quality and quantity of the personal data involved (i.e., when larger and more complicated personal data is involved, stricter measures should be adopted).

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

The PDPA does not require reporting data breaches to relevant data protection authorities.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

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.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/ Administrative Sanction	Criminal Sanction
Access premises, acquire information, copy and retain documents and other objects.	Monetary damages based on the amount of a data subject's actual loss.	Prison sentence of up to five years and/ or criminal fine of up to NT$1 million for: (i) illegal collection, processing or use of personal data with an intention to make unlawful profit, causing injury to another; (ii) failure to obey a central government authority's order imposing restrictions on cross-border transfers of personal data with an intention to make unlawful profit, causing injury to another; or (iii) illegal change or deletion of personal data files or employment of any other illegal means with an intention 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.
Rectification orders.	The courts may set the amount of damages at NT$500 to NT$20,000 for each incident per person if a data subject cannot prove the amount of actual damages or compensation.	Prison sentence of up to two years and/ or criminal fine of up to NT$200,000 for: (i) illegal collection, processing or use of personal data, causing injury to another; or (ii) failure to obey a central government authority's order imposing restrictions on cross-border transfers of personal data, causing injury to another.
Administrative fine of up to NT$500,000, which may be imposed consecutively until the violation is rectified.		

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

Both the central and local government authorities have the power to carry out audits and inspections on the non-government agencies. In order to audit and inspect any non-compliance, they may access the premises of non-government agencies, require information, and copy and retain documents and other objects. If a non-government agency is found in violation of the PDPA, the authorities may impose an administrative fine and take any of the following actions: (i) prohibit the violating non-government agency from collecting, processing or using the personal data; (ii) demand the deletion of the personal data files already processed; (iii) confiscate or destroy the personal data illegally collected; and (iv) publicise the violation case, the name of the non-government agency, and the name of the person in charge.

Most cases are related to financial institutions. Several financial institutions were given administrative fines for breach of confidentiality or unauthorised disclosure of customers' data. In one case, a bank was fined because it failed to take necessary protective measures when uploading its files to a search engine, causing its customers' data to be accessed by the general public online. In the cases involving financial institutions, the FSC imposed administrative fines or sanctions in accordance with the law governing the specific industry, such as banking law or insurance law. No penalties or sanctions stipulated under the PDPA were imposed.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within Taiwan respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Disclosure and transfer of personal data to foreign law enforcement agencies constitute the use of the personal data for a new purpose and thus require a valid legal basis for the disclosure (e.g., the use that is specifically permitted by law or data subjects' separate written consent). Most companies in Taiwan will reject such disclosure unless foreign law enforcement agencies have a Taiwanese court

serve the request through judicial assistance because under such circumstances, the companies may disclose the personal data as the disclosure is permitted by law.

15.2 What guidance has the data protection authority(ies) issued?

The MoJ has not issued any guidance on this issue.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The PDPA took effect on 1 October 2012. Although the MoJ has issued rulings from time to time in response to various inquiries from the government agencies and non-government agencies, the rigidity of enforcement varies among different industries. For those that have been subject to the Computer-processed Personal Data Protection Act prior to 1 October 2012, such as financial institutions, the Financial Supervisory Commission has required such institutions to conduct personal data inventory checks and internal audits and continues to impose fines on those that are not in compliance with the PDPA. As for the industries that were not subject to the Computer-processed Personal Data Protection Act prior to 1 October 2012, the regulators are still busy educating those industries about the requirements of the PDPA.

On the other hand, data subjects' awareness of their rights to the personal data has been enhanced after the PDPA took effect. On 20 October 2014, the Taipei District Court granted a consumer's claim of NT$500 for non-pecuniary damage to his privacy. The case involved an APP service provider and a mobile operator which provides a social networking APP that allows users to identify their contact persons' mobile operators, based on which users know whether they and the persons in their address books choose the same mobile operator and whether they are entitled to lower mobile phone charges for calls with those in their address books. The court confirmed that the consumer's choice of mobile operator, when associated with his name, is his personal data and may not be disclosed to others without the consumer's written consent. The court ruled that the APP service provider and the mobile operator that provides the APP should be jointly and severally liable for causing damage to the consumer's moral right by illegally using his personal data without his written consent. According to the news report, the APP service provider and the mobile operator have decided to appeal against this court judgment.

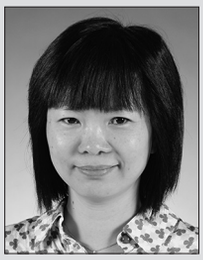
16.2 What "hot topics" are currently a focus for the data protection regulator?

The unauthorised disclosure of personal data via smart phones is a hot topic for the data protection authorities. The NCC has been testing various popular smart phones in the market because the media reported that the personal data contained in smart phones will be accessed by and disclosed to mobile manufacturers, mobile operators, and APP service providers without the relevant data subjects' consent. According to the news report, the NCC plans to invite mobile manufacturers to verify the testing results and suggest that they imbed appropriate security mechanisms in mobile phones in order to enhance the safety of data transmission.

Ken-Ying Tseng
Lee and Li, Attorneys-at-Law
9F, 201 Tun Hua N. Road
Taipei
Taiwan 10508, R. O. C.

Tel: *+886 2 2183 2179*
Fax: *+886 2 2713 3966*
Email: *kenying@leeandli.com*
URL: *www.leeandli.com*

Ken-Ying Tseng formed and leads the Personal Data Protection Practice Group at Lee and Li. She has been frequently invited to deliver speeches on the compliance of new Personal Data Protection Act both in Taiwan and overseas and has published numerous articles in local and international publications. She constantly advises clients, mostly multinational companies, on the areas of personal data protection, privacy, data security, cross-border data transfer, telemarketing/e-marketing, sweepstakes, online game, and electronic signature, as well as other e-commerce or Internet related matters. Ken-Ying has been nominated as an Internet, e-commerce and data protection expert by Who's Who Legal since 2012. She was named a Leading Mergers and Acquisitions Lawyer by Asialaw in 2013 and 2014 and a Leading Lawyer by IFLR 1000 in 2014.



Rebecca Hsiao
Lee and Li, Attorneys-at-Law
9F, 201 Tun Hua N. Road
Taipei
Taiwan 10508, R. O. C.

Tel: *+886 2 2183 2257*
Fax: *+886 2 2713 3966*
Email: *rebeccahsiao@leeandli.com*
URL: *www.leeandli.com*

Rebecca Hsiao is the key member of the Personal Data Protection Practice Group at Lee and Li and practices in the areas of privacy and consumer protection, antitrust and competition law, mergers and acquisitions, securities, and corporate and investment laws. She has constantly advised clients on the compliance of the personal data protection law and delivered speeches on this topic to various government and non-government clients.

理律法律事務所
LEE AND LI
ATTORNEYS-AT-LAW

Lee and Li is a full-service law firm and the largest law firm in Taiwan. Its history can be traced back to the 1940s. As of today, Lee and Li has formed practice groups which span corporate and investment, banking and capital markets, trademark and copyright, patent and technology, and litigation and ADR. Its services are performed by over 100 lawyers admitted in Taiwan and more than 100 technology experts, patent agents, patent attorneys, and trademark attorneys. Lee and Li was awarded the Taiwan Firm of the Year by IFLR from 2001 through to 2013 and named the Taiwan Deal Firm of the Year in 2005, 2007, 2009, 2010, 2011, and 2012 by ALB in the field of Capital Market and M&A. In 2012, Lawyers World Magazine ranked Lee and Li the Global Leading Firm. In 2012 and 2013, China Law & Practice awarded Lee and Li the "Taiwan Firm of the Year".

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Litigation & Dispute Resolution
- Lending & Secured Finance
- Merger Control
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

GLG
Global Legal Group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk

"This article appeared in the 2015 edition of The International Comparative Legal Guide to: Data Protection; published by Global Legal Group Ltd, London." (please hyperlink www.iclg.co.uk)