Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Data Protection & Privacy 2022

Taiwan: Law & Practice
Che-Hung Chen, Doris Lu, Jakob Huang and Ting-Yi Chen
Chen & Lin

practiceguides.chambers.com

TAIWAN

Law and Practice

Contributed by:
Che-Hung Chen, Doris Lu, Jakob Huang and Ting-Yi Chen
Chen & Lin see p.23

CONTENTS

1. BASIC NATIONAL REGIME

1.1 Laws

The Personal Data Protection Act (PDPA) is the primary law regulating personal data protection. It was first enacted in August 1995, as the Computer-Process Personal Data Act, and regulated governmental agencies and certain private sectors. The PDPA has been effective since 1 October 2012, and regulates any person – including governmental agencies and all private sector entities – who collects, processes or uses personal data. Privacy and personal data protection are related to the constitutional protection of privacy.

In addition to the PDPA, the Legislative Yuan has also enacted certain special data protection requirements in some sector-specific laws, such as the Insurance Act, the Financial Holding Company Act, the Banking Act, the Human Biobank Management Act, the Pharmaceutical Affairs Act and the National Sports Act.

Furthermore, the Trade Secrets Act may apply if the trade secrets of an enterprise are involved. If an offence against computer security is involved, then the criminal sanction of the Criminal Code of the Republic of China may apply. If any national security issue is involved, the National Security Act may apply.

There is no single specific law in Taiwan that regulates all the sensitive digital technologies like artificial intelligence. On the contrary, the different sector-specific laws will catch and govern different aspects and applications of sensitive digital technology, like artificial intelligence. Recently, certain legislators have proposed amendments to the PDPA to update and strengthen data protection in the digital industry environment. The Executive Yuan proposed the establishment of a Digital Development Ministry to govern digital technology and data protection and cybersecurity in the digital environment. The Digital Development Ministry may propose more implementation rules to enhance the regulation of sensitive digital technology in more detail.

1.2 Regulators

The Ministry of Justice (MOJ) is the main regulator for personal data protection and is in charge of proposing the draft bill of the PDPA, promulgating the Enforcement Rules of the PDPA and issuing various interpretations to answer questions in respect of compliance with the PDPA.

The enforcement of the PDPA is administered by the central governmental authorities that supervise the business operation of non-governmental agencies and local government authorities. Both central and local governmental authorities have the power to:

- carry out audits and inspections on non-governmental agencies;
- request information;
- demand rectification; and
- impose administrative penalties against non-governmental agencies for non-compliance with the PDPA.

1.3 Administration and Enforcement Process

Under the PDPA, central and local governmental authorities have the power to conduct an audit and inspection on non-governmental agencies, for which they may access the premises of non-governmental agencies, require information, and copy and retain documents. If the non-governmental agency refuses to provide the information and documents, the authorities may – to the extent of least harm – adopt compulsory measures to obtain such information and documents. The non-governmental agency may raise an objection against such compulsory measures. However, if the governmental authority refuses

to change such compulsory measures, the non-governmental agency may only argue against such compulsory measures in the proceeding in which it argues the administrative decision on the merits.

Except for the foregoing investigation procedure and the procedural complaint procedure, there are no special procedures regulating the administrative process in respect of investigations and penalties imposed, and the respondent's due process and appeal rights and procedures. The general administrative laws will govern, such as the Administrative Procedure Act, the Administrative Appeal Act and the Code of Administrative Procedure.

1.4 Multilateral and Subnational Issues

The national system in respect of data protection adopts an "APEC-EU referential" approach. The meeting minutes of the Executive Yuan in connection with the approval to submit the draft bill of the PDPA to the Legislative Yuan addressed that the PDPA incorporates certain provisions under Directive 95/46/EC. As one of APEC's member economies, Taiwan has executed the APEC Privacy Framework, which indicates nine principles in respect of privacy protection; the PDPA also incorporates the principles guided by the APEC Privacy Framework.

In 2011, APEC developed the Cross-Border Privacy Rules (CBPR) system, under which companies trading within the member economies develop their own internal business rules consistent with the APEC privacy principles to secure cross-border data privacy. Taiwan joined the CBPR system in December 2018, with the Institution for Information Industry applying to be the Accountability Agent under the system. In June 2021, the Institute for Information Industry was appointed by APEC as the Accountability Agent for CBPR verification in Taiwan for domestic enterprises.

Furthermore, to seek an "adequacy decision" from the European Commission, the Personal Data Protection Office has filed the evaluation reports required for GDPR adequacy status; the application is still under review and discussion. All major laws regulating privacy and personal data protection are at the national level. The relevant regulations at the subnational level are solely relevant to the implementation of those national laws and regulations by the different functioning bureaus of local government.

1.5 Major NGOs and Self-Regulatory Organisations

NGOs

The major privacy or data protection NGOs include:

- the Data Protection Association of the Republic of China, which focuses on promoting cybersecurity and data protection by way of giving data protection lectures, advising on encryption methods and providing a data protection consultation service; and
- the Taiwan Association for Human Rights, an independent NGO focusing on human rights protection, including privacy and personal data protection, by way of policy watching, monitoring and advocacy.

Industry Self-Regulatory Organisations (SROs)

Certain SROs in specific industries, particularly the financial industry, provide guidance to their members in connection with data protection, confidentiality and cybersecurity. For example, the Bankers Association of the Republic of China provides guidance that advises members to take certain data protection measures, including maintaining the confidentiality of clients' information, establishing safety control mechanisms for data protection and reporting any data breaches to the competent authority pursuant to the laws and regulations. The Life Insurance

Association of the Republic of China and the Non-Life Insurance Association of the Republic of China provide self-regulatory rules on handling cybersecurity and data protection, requiring members to do the following, for example:

- adopt rules regarding the use of mobile devices (including "bring your own device") and social network media, and rules regarding the use of cloud services;
- establish cybersecurity and data protection mechanisms pursuant to the evaluation principles set forth in the self-regulatory rules;
- establish app cybersecurity control and management mechanisms pursuant to the operation principles set forth in the self-regulatory rules; and
- adopt equipment scrapped procedures (ie, the procedure that shall be followed when disposing of equipment) so as to ensure that confidential and sensitive information is removed and that the data stored in the hard drive may not be recovered.

The self-regulatory rules further provide that the contents thereof shall be incorporated into the internal audit and control system, and that compliance reviews shall be conducted periodically.

1.6 System Characteristics

Taiwan adopts the civil law system, and most primary and general laws and regulations follow the laws and regulations of other civil law countries, such as Japan. On the other hand, quite a few laws and regulations regarding modern technology follow US and EU laws. Such a multiple-reference approach is reflected in various laws and regulations, as well as the interpretations thereof. Due to this, it is difficult to state whether Taiwan data protection and cybersecurity procedures follow any single specific model.

As noted in **1.2 Regulators**, the enforcement of the PDPA is administered by central relevant business governmental authorities and local governmental authorities, rather than by any single governmental authority. It is difficult to obtain a whole picture in respect of the enforcement status of different central and local governmental authorities, since they are not subject to mandatory public disclosure requirements. Given the absence of sufficient available public information, Taiwan does not have a proper basis upon which to note that the enforcement is relatively aggressive or less so. However, based on the limited public information available, enforcement in respect of data protection by the Financial Supervisory Commission (FSC) will be relatively aggressive compared to other governmental authorities.

1.7 Key Developments

Guidelines for the Collection of Personal Data for COVID-19-Related Investigations

As the COVID-19 health crisis evolves, the Taiwan government has taken several measures to contain and mitigate the threats of the virus. These measures involve the processing of different types of personal data. In order to balance privacy with health and security, the Central Epidemic Command Center (CECC) released guidelines for the collection of personal data by public venues for health authorities to use if needed for COVID-19-related investigations. According to these guidelines, the data subjects should be informed of what type of information is being collected, its purpose, the person or entity responsible for its collection, and how the information is to be used, among other matters. The purpose of collection shall be "public sanitation and prevention of communicable disease", and the collected data shall not be used outside of such specific purpose. If necessary for the purpose of pandemic prevention, the data can be provided to sanitary authorities to conduct the pandemic investigation and to contact individuals in accordance with the Communicable Disease Control Act.

All information should be kept confidential and deleted after 28 days; the record of the deletion of items and dates shall also be preserved. If the personal data is collected by electronic methods, the information security protection procedure shall also be implemented to ensure that the personal data will not be infringed.

Furthermore, even though there are some arguments regarding vaccine passport in other countries, the CECC launched a digital vaccine passport in January 2022 in order to control the spread of the virus. The CECC has announced that vaccine records, such as the vaccine passport or the vaccine record yellow card, will be required when people would like to enter certain places of leisure and entertainment, such as concert halls, dance halls and nightclubs; they are also required when entering hospitals and nursing homes, etc. Certain arguments have indicated that such measures shall be subject to clear statutory authorisation, but the CECC has planned to rely on the broad and general authorisation under the Communicable Disease Control Act.

New Draft of Technological Investigations Act Proposed

Modern technology is becoming almost inseparable from citizens' daily lives, as it makes life convenient, but it can also be exploited by malign entities. For example, criminals could use smartphones to obtain illegal information, encrypt data to hide it from authorities, transmit data through instant messaging, or trade narcotics with e-payment services. Modern crime detection law enforcement officers are facing difficulties as criminals quickly adapt their methods to exploit new technology and equipment in ways that are not yet addressed under the law.

In response to these issues, the MOJ has proposed a draft "Technological Investigation Act" to deal with new forms of digital crimes by providing law enforcement agencies with tools powered by new technologies.

Under this Act, the scope of "privacy space" is narrowed, and the prosecutor may use technological equipment or techniques to investigate people and items in the "non-privacy space" when necessary. Furthermore, the prosecutor can use GPS (Global Positioning System) or other location-tracking technologies to conduct an investigation, without the court's approval, if the period of such investigation is within two months. The record of investigation can be preserved for five years. Also, the prosecutor can install monitoring equipment on the cellphone of a person under surveillance, or hack into their cellphone or computer.

This draft has drawn criticism, with some opponents expressing concern about the pervasive surveillance of interpersonal communications, and that people will live under constant surveillance by the government's judicial agencies.

The MOJ has stated that this draft is still under review, and the opinions from different perspectives will be taken into account in future revisions thereof. The Legislative Yuan has held a public hearing on the topic of "Human Rights Controversies Caused by Technological Investigation Techniques", discussing the potential issues and seeking balance between the measures under the draft Act and the protection of human rights. There has not yet been any substantial progress in this draft.

Proposed Amendments to Criminal Code – Deepfakes

The Criminal Investigation Bureau announced in October 2021 that it had uncovered alleged suspects using "deepfakes" to produce celebrity face-swapping porn and sell it for profit, making profits of more than TWD10 million in just one year. "Deepfakes" were also found to be

used in other crimes, such as making fake news to mislead the public in relation to the government's efforts to prevent and control the spread of the pandemic. The MOJ has proposed draft amendments to the Criminal Code, adding the offences of "making or distributing fictitious videos" and "making or spreading fictitious activities, statements, or conversations by others", etc. Furthermore, as deepfake videos may be disseminated swiftly on the internet or social media, the National Communications Commission is discussing amendments to the Digital Communications Act, which aim to set up certain measures to prevent the dissemination of deepfake videos, such as enabling the governmental agency to demand the internet service provider or social media operator to take down any deepfake videos immediately in certain specific circumstances.

1.8 Significant Pending Changes, Hot Topics and Issues

The Changeover of New Electronic Identification Cards

The Ministry of the Interior has proposed a plan to change over the new electronic identification card, but said plan raises continuous criticism and concerns. Given this, the Ministry of the Interior announced in January 2021 that the plan would be temporarily suspended, and might be resumed after the draft of a special law is proposed, based on further detailed discussion to reflect social consensus.

Academics call for law regulating controversial electronic identification card

Academia Sinica Information Law Center has proposed a report regarding the changeover of the electronic identification card, stating the following major concerns.

- The ill-prepared introduction of the new electronic identification card might lead to "immediate and serious threats" to the nation's democratic system, and the mandated adoption of the card might be unconstitutional, with a lack of accountability concerning the "smart government" plan, of which the electronic identification card would be part.
- The information security for the electronic identification card is insufficient. The Ministry of the Interior emphasised that the chips would be produced by domestic manufacturers, but lacked oversight over other technical systems. It has outsourced chip design, the development of the operating system and the manufacturing of chip-writing equipment, data application software and other features, threatening the security of the entire system. The two contractors in charge of chip design, blank card manufacturing and providing data-writing equipment to the Central Engraving and Printing Plant had allegedly undertaken significant work for Chinese financial agencies. Also, the design of the chip module and operating system, as well as the manufacturing of the data-writing equipment, might be done at overseas factories that have ambiguous ties to the Chinese government. The fact that the wafers are produced by Taiwan Semiconductor Manufacturing Co. does not eliminate such risk.
- The report also raised concern over the surveillance threat inherent to digitisation, saying that the nation's current laws governing information security are insufficient to meet the challenges that might arise.
- Lastly, the report recommended that the government should postpone the electronic identification card plan until these privacy and security issues have been properly addressed. The Ministry of the Interior shall establish the legal ground for the digitalising of the identification card, safeguarding individuals' rights, and ensuring that information security is well protected with appropriate legislation.

Lawsuit aims to press government to halt electronic identification card plan

In addition to the above, more than 50 professionals, led by the Taiwan Association for Human Rights, filed a suit against the Ministry of the Interior in November 2020, demanding stronger data protection and privacy measures ahead of the roll-out of electronic identification cards nationwide in 2021. This move is part of an initiative to fight for stronger protection of data and privacy before the official launch of the electronic identification card. The civic group has chosen to enter into legal proceedings to press the Ministry of the Interior to clearly address the stated concerns. As of January 2022, the litigation is still pending in the court and the electronic identification card has not yet been officially launched.

Controversial Electronic Fence System against COVID-19

In order to deal with the COVID-19 pandemic, the Taiwan government adapted a mobile phone-based "electronic fence" that uses location tracking to ensure that people who are quarantined stay in their homes or the hotels or premises designated for quarantine.

The Center of Disease Control sends the mobile phone numbers of the people who are quarantined to the telecommunication service providers every day, and these service providers upload the mobile phone location to the electronic platform. If the people who are quarantined leave the certain limited area, or turn the mobile phone off, the system would send a "warning message" to such person and the monitoring authority. Officials also call those quarantined people twice a day to ensure they do not avoid being tracked by leaving their phones at home.

Although this system has earned global praise, there are some complaints regarding its intrusiveness, with some critics claiming that using mobile phone signals to locate citizens may be unconstitutional, and that the statutory authorisation basis is not sufficiently clear.

This electronic fence system also applies to monitoring people observing self-health management (Digital Fencing 2.0) to prevent such persons going near large-scale events. At the end of 2020, the electronic fence system enabled the authority to find some people under self-health management violating the regulations by attending a new year's eve party. In response to the backlash, the authority further emphasised that this system does not monitor all people, but only applies to people under quarantine or self-health management, and all the data will be destroyed after 28 days. In addition, the authority stated that it has the necessary authorisation from the Communicable Disease Control Act and the Special Act for Prevention, Relief and Revitalisation Measures for Severe Pneumonia with Novel Pathogens, and that this system is the least intrusive means to prevent the spread of the virus and thus is not against the Constitution.

Due to the continuance of the COVID-19 pandemic, the electronic fence system remains in place despite the mentioned human rights issues, and the competent authority has detected violations of quarantine and self-health management rules and imposed administrative punishments therefor.

2. FUNDAMENTAL LAWS

2.1 Omnibus Laws and General Requirements

It is not a mandatory requirement to appoint a data protection officer. The Enforcement Rules of the PDPA suggest that data protection personnel shall be allocated, and indicate that it will be one of the approaches to establish the appropriate data protection measures. However,

according to the PDPA, governmental agencies shall assign data protection personnel when they keep personal data.

According to the PDPA, the collecting and processing of personal data (except sensitive personal data) shall be with and within the specified purpose, and shall meet any of the following statutory matters:

- it is based on any other law that specifically provides that the data collector can collect personal data without consent;
- it is based on any contractual or quasi-contractual relationship between the data collector and the data subject;
- the data subject voluntarily makes the personal data public;
- it is necessary for statistical or academic research by an academic research institute for the purpose of public interest, and the personal data is processed or disclosed in a manner that does not permit the identification of the data subject;
- it is based on the consent of the data subject;
- it is necessary for the public interest;
- the personal data is obtained from a generally accessible source, unless the interest of the data subject takes priority over that of the data collector or data controller; and
- the personal data collection and processing do not harm the rights and interests of the data subject.

As noted above, certain sector-specific laws and regulations or guidance promulgated by the associations of specific industries provide the standards in respect of establishing cybersecurity systems that apply the concepts of "privacy by design" or "privacy by default".

Under the PDPA, governmental agencies and non-governmental agencies shall take appropriate data protection measures, which may include conducting privacy, fairness or legitimate impact analyses and other measures, such as preventing personal data from being stolen, altered, damaged, destroyed or disclosed. Furthermore, the relevant business governmental authority may designate a non-governmental agency to set up a plan of security measures for the personal data or the disposal measures for the personal data upon the termination of business.

According to the PDPA, the data subject shall have the following rights:

- to access his or her personal data that has been collected;
- to copy his or her personal data files;
- to supplement or correct his or her personal data that has been collected;
- to object to the collection, processing and use of his or her personal data; and
- to request the deletion of his or her personal data that has been collected.

Any advance waiver of such rights by the data subject will be null and void.

The governmental agency or the non-governmental agency should ensure the accuracy of personal information and correct or supplement it, either ex officio/at its discretion or upon a request from the data subject. The governmental agency or non-governmental agency should – again, either ex officio/at its discretion or upon a request from the data subject – delete the personal data or discontinue the collection, processing or use of personal data in the following circumstances:

- when the purpose of such data collection no longer exists or the stated time period expires, unless it is necessary for the performance of an official duty or the fulfilment of a legal obligation and has been recorded, or

when it is agreed by the data subject in writing; or
- when the collection, processing or use of such data violates the PDPA.

Under the PDPA, personal data could be used when it is necessary for a governmental agency or academic institute to perform statistical or other academic research only after anonymisation, de-identification and pseudonymisation. There is no law or regulation specifically regulating emerging technologies, such as profiling, microtargeting, automated decision-making, online monitoring or tracking, big data analysis or artificial intelligence. Nevertheless, in the cases relevant to these emerging technologies, current laws may apply (eg, the PDPA and the Criminal Code), depending on the legal issues involved.

The PDPA aims to prevent harm on personality rights, which includes reputation and privacy. Therefore, the concepts of "injury" or "harm" under the PDPA include pecuniary damages and non-pecuniary damages. Also, if there is infringement to reputation, a proper rehabilitation action may be requested.

2.2 Sectoral and Special Issues

Under the PDPA, "sensitive data" is defined as personal data regarding medical records, medical treatment, genetic information, sexual life, health examinations and criminal record. Such sensitive data shall not be collected, processed or used unless the statutory requirements are satisfied, such as compliance with the laws and regulations, and obtaining written consent from the data subject.

Financial Data

Financial conditions fall within the definition of personal data under the PDPA, and the PDPA will apply thereto. Furthermore, under the Banking Act, a bank shall keep customer information and related information on the deposits, loans or remittances of its customers and transaction materials in confidence.

Health Data

As noted above, medical records and health examination records fall within the definition of personal data under the PDPA, and the PDPA will apply. Furthermore, according to the National Health Insurance Act, the insurer (ie, the Bureau of National Health Insurance of the Ministry of Health and Welfare) may require hospitals to provide certain personal data that is necessary for the insurer to carry out and administer the business of national health insurance. The obtaining of information by the insurer in accordance with the above, and the storage and use of such information, should comply with the PDPA.

During 2018, the National Health Insurance Administration adopted a cloud-based medical records management platform, which aims to enable physicians to better understand a patient's condition and quickly deliver suitable services during regular and emergency visits by accessing historical diagnoses, test results and treatments saved on the cloud system. According to the National Health Insurance Act and Regulations Governing the Production and Issuance of the National Health Insurance IC Card and Data Storage, medical care institutions shall access medical records stored in or uploaded through National Health Insurance IC Cards when providing medical services for patients based on medical needs. Therefore, since it is expressly required by law and is within the necessary scope for the National Health Insurance Administration to perform its statutory duties, the processing and use of medical records stored in the cloud system are in accordance with the PDPA.

Communications Data

There is no specific law in Taiwan directly addressing the general and primary rules governing any specific communication data, such as voice telephony, internet or social media. If the content involves personal data collection, processing and use shall be in compliance with the PDPA. If it involves certain specific offences or serious crimes, the Communication Security and Surveillance Act will govern, under which a warrant issued by the court will be required for obtaining the communication data of suspects or defendants.

The issue of the right to be forgotten was once discussed by the court. In a Taiwan Taipei District Court case (case No 104-Su-Geng-Yi-Zi-31), the plaintiff (the former CEO of a professional baseball team) was charged with the offence of fraud due to alleged involvement in a match-fixing scandal. At the end, the court rendered a judgment of not guilty. The individual then took legal action against a famous internet search engine, claiming that it should take down certain search results, which he claimed infringed his right of privacy, his reputation and his right to be forgotten. Given the absence of a statutory provision directly addressing the right to be forgotten, the court discussed and interpreted the right to be forgotten based on the concept of the right of privacy. The court indicated that the match-fixing scandal involved the public interest and, furthermore, that the use of such information did not violate the PDPA since it was obtained from publicly available resources. Although such public information may impose certain restrictions on the plaintiff, such restrictions could be justified, since keeping such information publicly available will be in the public interest. A Supreme Court judgment (case No 109-Tai-Shang-Zi-1015) adopted a different view and stated that the internet platform provider is obliged to examine the content if a user notifies the internet platform provider of the infringing content and request for removal. If there are reasons to believe the user's assertion, the internet platform provider is obliged to take prevention measures in order to suspend the infringement, such as taking down the infringing content. Otherwise, the internet platform provider may be treated as an accomplice in the infringement of other's rights.

From these judicial judgments, it is obvious that the courts will make decisions on a case-by-case basis, based on the impact of the content being kept on the internet search engine or social media and the protection of public interest.

Children's Privacy

Names, faces, characteristics and other personal identification information relate to the privacy of children and constitute personal data, so the PDPA will apply thereto. In 2017, a parent child-life blogger uploaded a video on Facebook that showed her harshly dressing down her four-year-old daughter, who cried and confessed her wrongdoing. This video caught the public attention and the blogger was blamed by the public for disregarding her child's privacy. However, there has not yet been any case in which a child has sued a parent for infringement of his or her privacy or personal data protection in Taiwan.

The Protection of Children and Youths Welfare and Rights Act regulates the confidentiality requirement for the case files and personal data of children and youths who are subject to special treatment under the act, as well as the information of their families. Furthermore, the act prohibits certain information in respect of children and youths – such as criminal cases and drug abuse – from being disclosed by promotional material or on TV, the internet, other media or public channels. Failure to comply with the act may result in administrative fines.

Given that children are exposed under online privacy/harmful information threats, a draft "Children's Internet Personal Data Protection Act" was proposed in March 2020, to strengthen the protection of children's data online. Under this draft, internet operators shall take reasonable measures to protect the confidentiality, safety and completeness of children's data, and the violator is subject to punitive damages of ten times the actual damages.

Students' Data

More and more universities and high schools are implementing face recognition systems to track students' class attendance or to allow access to the library by scanning students' faces at the entrance and exit points. Nevertheless, critics worry that the excessive use of this technology could turn into the surveillance of students. The Ministry of Education has stipulated a guideline of personal data protection for schools using biometric characteristics recognition techniques. In addition to restating that the collection and use of personal data collected by the biometric characteristics recognition techniques shall be subject to the PDPA, the guideline stipulates that the original biometric characteristics data shall not be preserved unless necessary, and the collected personal data shall be pseudonymised.

2.3 Online Marketing

The PDPA regulates the collection and use of personal data for marketing purposes. When a non-governmental agency uses personal information for the purpose of marketing but the data subject refused the marketing, such marketing shall stop immediately. Also, the non-governmental agency shall offer ways for the data subject to express his or her refusal at the time such marketing first appears in public, and shall compensate any necessary cost and expense to express such refusal.

Moreover, the Financial Holding Company Act provides that financial holding companies' subsidiaries engaging in co-selling activities among themselves shall apply to the FSC for prior approval and make sure that such activities will not harm the interests of customers. The subsidiaries of the financial holding company shall comply with the provisions of the PDPA with regard to the joint collection, processing and use of the basic personal data and dealing or transaction records of customers.

There is no specific law in Taiwan that directly addresses the general and primary rules regulating all types of online marketing. Nevertheless, for electronic marketing, the Consumer Protection Committee has promulgated guidance advising that the enterprises shall collect and use consumers' personal information in accordance with laws, and provide reasonable protective measures.

2.4 Workplace Privacy

In Taiwan, issues relevant to workplace privacy focus mainly on email monitoring.

In most cases, the Taiwan court uses two standards to determine whether email monitoring is in violation of employees' privacy rights, as follows:

- whether the employees have a reasonable privacy expectation for these emails; and
- if there is no reasonable privacy expectation, whether it is prohibited by law for employers to monitor employees' emails.

The concept of "reasonable privacy expectation" is based on Article 3 of the Communication Security and Surveillance Act, which provides that the communications under surveillance are limited to those that have content that may reasonably be expected to be private or secret by the persons who are monitored, with sufficient

factual support. Some court rulings further point out that if the company has an email policy in place and has explicitly stated that employees' emails would be monitored, or if the employees have signed written consent for email monitoring, then it is hard to say that the employees have a reasonable expectation of privacy for such emails.

Whistle-Blowing

According to the Labour Standards Act, upon the discovery of any violation by the business entity of labour laws or administrative regulations, an employee may file a complaint with the employer, the competent authorities or the inspection agencies. The employer cannot then terminate the employment relationship, change the employment terms and conditions, reduce the wages or the rights and other benefits, or take any unfavourable measure against such employee. If the employer violates any of these prohibitions, such action shall be null and void.

Also, the competent authority receiving the complaint shall keep the identity of the complainant in confidence, and shall not disclose any information that might reveal it. Any authority that violates this shall be liable for damages so caused to the complainant. In addition, public officials shall be held liable under criminal and administrative laws.

2.5 Enforcement and Litigation

There are criminal liabilities and administrative liabilities under the PDPA. The standard for conviction in a criminal proceeding is "beyond a reasonable doubt" – ie, the prosecutor must present evidence that is credible and sufficient to prove that no reasonable doubt exists against the guilty judgment to the defendant. Regarding administrative sanctions, the governing authority must prove that an act in breach of duty under the PDPA has been committed intentionally or negligently.

Enforcement Penalties

The criminal penalties for violation of the PDPA include imprisonment for not more than five years, or criminal fines of not more than TWD1 million, or both.

The administrative penalties for violation of the PDPA are administrative fines of no less than TWD20,000 but no more than TWD500,000. The legal representative, manager or other representatives of a non-governmental agency may be subject to the same fines when the non-governmental agency receives an administrative fine.

If there are any other violations of other criminal laws or administrative laws or regulations, criminal or administrative penalties in accordance with such laws or regulations would be imposed.

Recent Enforcement Cases

In January 2022, Fuwan Insurance Broker Company was fined TWD300,000 by the FSC, for failing to effectively manage the collection, processing and use of personal data by its insurance agents, in violation of Article 19, Paragraph 1 and Article 20, Paragraph 1 of the PDPA.

Private Litigation

In general, the burden of proof in civil litigation shall be borne by the plaintiff, who is obliged to establish all the requisite elements of a case, through evidence. Therefore, if the plaintiff filed a lawsuit for alleged privacy or data infringement under the civil code, the burden of proof is borne by the plaintiff, who has to establish that the defendant has wrongfully damaged the plaintiff's rights intentionally or negligently, and that injuries have arisen therefrom.

Nevertheless, the PDPA has special rules for the plaintiff's burden of proof in a civil case under the PDPA, under which the law lifts a certain burden of proof from the plaintiff. Therefore, once the

plaintiff has met his or her burden of proof by establishing the infringement of his or her rights from a non-governmental agency's illegal collection, processing and use of personal information, or other ways of infringement due to violations of the PDPA, the burden of proof shifts to the defendant to show that such action was unintentional or non-negligent.

If the plaintiff has proved that a governmental agency infringes the rights of personal data due to violations of the PDPA and that there are injuries arising therefrom, the governmental agency should be liable for damages and compensation, unless it can prove that the damages were caused by natural disaster, incident or other force majeure.

Class Actions

Class actions are allowed in Taiwan. For cases caused by the same cause and fact, and where multiple data subjects are infringed, the organisations regulated by the PDPA may – after obtaining a written authorisation of litigation rights of 20 or more data subjects – represent such data subjects in bringing a lawsuit to the competent court by its own name.

The first data breach class action lawsuit was brought by the Consumers' Foundation against a travel agency for the alleged illegal disclosure of collected personal data in March 2018.

Major Cases (Private)

In a Taiwan High Court Case (case No 107-Shang-Yi-Zi-383), the plaintiff (a female successor of a large enterprise) claimed that the defendants (the plaintiff's ex-husband as well as a male successor of another larger enterprise and his lawyer and private detectives) should compensate her injuries for having used a GPS locator on her car to track her locations. The court opined that the plaintiff had a reasonable expectation of privacy for her movement and visiting places, even if she was in public places, so the defendants had violated the plaintiff's privacy by tracking her location without legitimate reasons using the GPS locator (the defendants explained they used the GPS locator due to the driver being under suspicion of drug abuse, but such explanation did not persuade the court). The defendants were ordered to compensate the plaintiff non-pecuniary damages of TWD250,000.

3. LAW ENFORCEMENT AND NATIONAL SECURITY ACCESS AND SURVEILLANCE

3.1 Laws and Standards for Access to Data for Serious Crimes

Under the Communication Security and Surveillance Act, a warrant from the competent court will generally be required in order to obtain data in criminal cases.

The Communication Security and Surveillance Act sets up certain safeguards to protection privacy, as detailed below.

- The enforcement authority shall file at least one report every 15 days during the period of communication surveillance, describing the progress of conducting the surveillance and/or whether it is necessary to continue the surveillance. The prosecutor or the judge issuing the warrant may also order the enforcement authority to submit a report at any time. If a situation arises where the surveillance should not be conducted continuously, the judge shall withdraw the warrant and discontinue the surveillance, at his or her discretion based on experience and logic.
- Surveillance devices shall not be installed or placed in a private residence.
- Content obtained from surveillance that is irrelevant to the purpose of the surveillance

shall not be included in the written record of such surveillance.
- Prior to the expiration of the communication surveillance, the surveillance activity should be halted immediately if it is deemed unnecessary by the prosecutor or the trial judge.
- When the communication surveillance ends, a notice will be provided to the person under surveillance stating the relevant information of the surveillance case and the case number of the authority issuing the warrant, the actual period of surveillance, whether communications information corresponding to the purpose of the surveillance has been obtained, and the remedy procedure.

3.2 Laws and Standards for Access to Data for National Security Purposes

When it is necessary to conduct surveillance on the domestic, cross-border or offshore communications of foreign forces or hostile foreign forces (or their agents) in order to collect intelligence on such forces – including organisations with the aim of operating international or cross-border terrorist activities – to protect national security, the head of the national security authority may issue a warrant to do so. If the subject under surveillance has household registration in Taiwan, the judicial approval level shall be escalated and prior approval from the judge of the High Court will be required. However, this restriction does not apply in the event of an emergency, in which case the national security authority should inform the competent High Court judge of the issuance of the warrant and obtain the permission ex post facto. If permission is not granted within 48 hours, the surveillance activity should be halted immediately.

The privacy safeguards are basically the same as for general criminal cases, provided that:

- the decision to halt or continue the surveillance will be made by the head of the national security authority; and
- the ex post written notice to the person under surveillance will only apply when the person under surveillance has household registration in Taiwan.

3.3 Invoking Foreign Government Obligations

In Taiwan, the feasible solution will be by way of judicial co-operation assistance, which shall be processed by the governmental judicial agencies. Taiwan has not signed the CLOUD Act agreement with the USA, but has signed agreements on mutual judicial co-operation in criminal matters with the USA, the Philippines, South Africa, China, Poland, the Republic of Nauru and Belize. Taiwan has also signed agreements on mutual judicial co-operation in civil matters with China and Vietnam. Under such agreements, an organisation invoking a foreign government access request may obtain and transfer personal data to foreign governmental agencies.

3.4 Key Privacy Issues, Conflicts and Public Debates

A recent case in which a judicial police officer applied a GPS locator on a suspect's car to investigate a smuggling case sparked public debate in connection with government access to personal data. It was debated whether prosecutors or judicial police officers could collect and use GPS records for investigation purposes. The court opined that GPS records were non-public activities of people and that, therefore, collecting or using such GPS records would infringe privacy rights. Since there was no statutory basis to collect and use GPS records to investigate crimes, there was no legal reason for prosecutors or judicial police officers to do so. However, some argued that such opinions would lead to difficulties in criminal investigations, and it was

suggested that the authorities should amend the relevant laws to keep up with new technology.

In September 2020, the MOJ proposed a Draft of Technological Investigations Act, empowering the authorities to exploit new technology and equipment to conduct investigation. This new draft has drawn some criticism and there is no specific timeframe for when it will be enacted (please see **1.7 Key Developments** for more details).

4. INTERNATIONAL CONSIDERATIONS

4.1 Restrictions on International Data Issues

Under the PDPA, the governmental authority in charge of the pertinent industry may limit international data transfers if:

- they involve important national interests;
- a national treaty or agreement specifies otherwise;
- the country receiving personal information lacks proper regulations towards the protection of personal information and it might harm the rights and interests of the data subject; or
- international transfers of personal information are made through an indirect method in which the provisions of the PDPA may not be applicable.

On 25 October 2012, the National Communications Commission issued an administrative rule stating that communications enterprises are prohibited from transferring their subscribers' personal data to China, since China lacks proper regulations towards personal data protection.

4.2 Mechanisms or Derogations that Apply to International Data Transfers

There are no specific mechanisms or derogations in Taiwan that apply to international data transfers.

4.3 Government Notifications and Approvals

If a financial institution would like to outsource its operations of data entry, processing and output of an information system related to consumer finance business to an offshore service provider, it must submit the documents to the FSC for approval.

4.4 Data Localisation Requirements

There is no data localisation requirement under Taiwan law.

4.5 Sharing Technical Details

No software code, algorithm or similar technical detail is required to be shared with the Taiwan government.

4.6 Limitations and Considerations

As noted above (see **3.3 Invoking Foreign Government Obligations**), the contractual parties shall provide judicial co-operation assistance under the judicial co-operation assistance agreements, pursuant to which an organisation may collect or transfer data.

4.7 "Blocking" Statutes

There is no concept of "blocking" in Taiwan.

5. EMERGING DIGITAL AND TECHNOLOGY ISSUES

5.1 Addressing Current Issues in Law

Most of the emerging technologies – such as big data analytics, automated decision-making, profiling or microtargeting, artificial intelligence, internet of things (IoT) or ubiquitous sensors,

facial recognition, drones and "dark patterns" or online manipulation – are not specifically addressed in the law or regulations. Depending on the legal issues involved, different laws or regulations may apply, including the PDPA, the Criminal Code and the Trade Secrets Act. However, developments in the following fields are worth noting.

In December 2018, a provision governing autonomous vehicles was added to the Regulations of Road Transportation Safety, according to which any enterprise or car research institute with a legal registration certificate may apply for a licence and road test for autonomous vehicles. Relevant road safety regulations shall be applicable to such autonomous driving.

Biometric Data

Biometric data is specifically regulated under the Human Biobank Management Act and the Regulations Governing the Collection, Management and Use of Individual Biometric Data.

The Human Biobank Management Act regulates the establishment, management and applications of the human biobank, and protects the rights of information privacy of biological database participants. Under the Human Biobank Management Act, a "human specimen" includes derivatives – such as cells, tissues, organs or bodily fluids – that are collected from a human body or produced by experimental operations and are sufficient to provide adequate information to identify the participant's biometrics. If the biometric data is stolen, leaked, tampered with or otherwise infringed, the operator of the biobank shall immediately investigate the matter, report it to the competent authority and notify the relevant participants in an appropriate manner. Personnel engaged in the collection, processing, storage or use of biological specimens shall not disclose any confidences or other personal data or information of the participant that is known or obtained as a result of their work.

The Regulations Governing the Collection, Management and Use of Individual Biometric Data, enacted in accordance with the Immigration Act, regulate the collection, management and use of fingerprints or facial characteristics for the National Immigration Agency of the Ministry of the Interior to recognise an individual when foreign people enter Taiwan or apply for residency or permanent residency. Those who obtain the data within the scope of their authority or employment shall maintain the confidentiality of such data, and shall be punished in accordance with the PDPA or relevant regulations if they violate this obligation.

In November 2017, a member of the Legislative Yuan proposed an amendment to revise the Household Registration Act, allowing the government to establish a database collecting a certain kind of biometric data of citizens for identification purposes (eg, the unique iris information of an individual). However, in Interpretation No 603, the Grand Justice held that fingerprints are important personal data, so are protected under rights of information privacy. Therefore, the government collecting the fingerprints of citizens without specifying the purposes of collecting such data in the Household Registration Act would be a violation of the constitution. According to this interpretation, the collection of an individual's iris information may also be in violation of the constitution if there is no law specifying the compelling public purposes of collecting such data.

Given the conclusion of Interpretation No 603, the proposal in November 2017 to establish a database collecting certain kinds of biometric data from citizens was heavily criticised, and the proposal was finally withdrawn.

Geolocation

There have been criminal cases where the defendants used GPS to record plaintiffs' locations and track vehicles. The issue involved therein was whether the drivers of the cars monitored by the GPS have reasonable privacy expectations. In those cases, the courts gave an affirmative answer because people could not tell where those cars on the road come from and go to, although they are seen on the road. Therefore, the drivers had reasonable privacy expectations for their movement. Accordingly, it would infringe the rights of privacy and may be in violation of the Criminal Code and the PDPA if someone uses GPS to track the movements of others.

Disinformation, Deepfakes or Other Online Harms

As fake news and disinformation spread more and more rapidly, they can influence users, manipulating them for political or economic reasons. To combat fake news and disinformation, relevant laws have been amended and sanctions on different types of fake news have been newly added. For example, sanctions on people who spread rumours or untrue information about "disasters" have been newly added to the Disaster Prevention and Protection Act. Similar sanctions on spreading fake news have also been added to the Food Administration Act, the Agricultural Products Market Transaction Act and the Act Governing Food Safety and Sanitation. Furthermore, the penalty for disseminating fake news concerning epidemic conditions of communicable diseases has been increased under the Communicable Disease Control Act.

The MOJ has proposed draft amendments to the Criminal Code to deal with deepfakes (see **1.7 Key Developments**). Furthermore, the legislators have proposed to amend certain laws, such as the Civil Servants Election and Recall Act and the Presidential and Vice Presidential Election and Recall Act, to impose more severe punishments for spreading fake news or fictitious images or video via digital technology.

Fiduciary Duty for Privacy or Data Protection

Neither the PDPA nor the Taiwan Company Act specifically provides that the violation of privacy or data protection will automatically constitute a breach of fiduciary duty; the matter is subject to the violation circumstance and would be determined by the competent court on a case-by-case basis.

5.2 "Digital Governance" or Fair Data Practice Review Boards

In Taiwan, the government is devoted to the establishment of "digital government". In 2007, the National Development Council outsourced the establishment of the Taiwan E-Governance Research Center (TEG), which seeks to systematically develop evaluation indices and databases of digital government-related planning and to promote a wide range of e-governance collaboration and international co-operation and alignment.

The missions of TEG include the following:

- research on prospective policies for digital governance;
- establishing a database for digital governance literature and survey data, which serves as a knowledge platform for easy access by both domestic and global communities and for facilitating knowledge exchange and sharing; and
- sharing research findings and experiences.

In the fifth phase of digital government (2017–2020), the goal was to achieve the three objectives of "providing people-centric convenient services", "implementing open, transparent and smart governance", and "optimising evidence-based effective policy".

The National Development Council has formulated the "Digital Government Programme 2.0 of Taiwan (2021–2025)" to accelerate various response measures to promote the government's digital transformation. The National Development Council will co-ordinate the implementation of various ministries, strengthen the transformation of cross-domain service processes from the needs of the people, and use a safe and reliable data transmission platform to share data across agencies. The government will continue its efforts in the following areas:

- accelerating the release of high-value data and facilitating the utilisation of such data;
- utilising the data of people's livelihood to optimise policies; and
- intensifying the service provided with new technology.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation.

The First Personal Data Infringement Class Action in Taiwan

The first personal data infringement class action was brought by the Consumers' Foundation against a travel agency in March 2018, with the court rendering its decision in October 2019.

In this case, the Consumers' Foundation claimed TWD4,509,575 compensation on behalf of 25 consumers, on the grounds that a travel agency leaked the personal data collected and thus caused damages to the consumers. The travel agency countered that the data breach was caused by a malicious hacking attack, and that it had notified the data subjects of the data breach after the occurrence of such attack; therefore, it should not be held liable for the data breach.

The court rendered a judgment in favour of the defendant, opining that the travel agency had established a security and maintenance plan for the protection of personal data files, and that it had conducted internal audits, education and training for cybersecurity personnel, and changed the passwords for the computer system periodically.

Therefore, although there was a data breach caused by a hacking attack, the court held that the travel agency was not in violation of the PDPA and thus should not be held liable for the data breach. The Consumer Foundation has filed an appeal against this judgment. During the procedure in the court of second instance, the Consumers' Foundation and the travel agency reached a settlement.

The First Grand Court Ruling Regarding the PDPA

In December 2020, the Grand Court made the first ruling regarding the PDPA.

The defendant had obtained the certificate of obligatory claim, the distribution table of compulsory enforcement and the stock report of his brother, and delivered such documentation to others. Since the defendant used the others' personal data illegally with the intention of impairing another person's interests, he was convicted of contravening Article 41 of the PDPA, which provides that "[I]f a person, with the intention of obtaining unlawful gains for himself/herself or a third party, or with the intention of impairing another person's interests, is in violation of Paragraph 1, Article 6, Articles 15, 16, 19, and Paragraph 1, Article 20, or an order or decision relating to the restrictions on cross-border transfers made by the central government authority in charge of the industry concerned in accordance with Article 21 of the PDPA, thereby causing damage to others, the person shall be sentenced to imprisonment for no more than five years; in addition thereto, a fine of no more than TWD1 million may be imposed."

The defendant filed an appeal to the Supreme Court, making a defence that "impairing another person's interest" in Article 41 of the PDPA should be limited to "property interests", and does not include non-property interests. Since the victim of the offence did not suffer any "property" damage, the defendant's act did not constitute the above-mentioned offence. The Supreme Court ruled that this legal issue should be submitted to the Grand Court, since it is arguable whether "impairing another person's interest" includes both property and non-property interests, and there were different opinions among the divisions of the Supreme Court.

The Grand Court made its decision on 9 December 2020, ruling that the "unlawful gains" referred to in "with the intention of obtaining unlawful gains for himself/herself or a third party" under Article 41 of the PDPA are limited to property interest, while the "interests" referred to in "with the intention of impairing another person's interests" under Article 41 of the PDPA shall include both property and non-property interests.

First Commercial Bank Data Breach

From May 2016, a criminal group made use of loopholes in the call recording system of First Commercial Bank's London branch to hack into its ATM system and insert malicious software therein. From 10–12 July 2016, members of the criminal group approached 21 ATMs in 22 branches of First Commercial Bank that had been targeted, collaborating with their accomplices overseas to withdraw more than TWD83.27 million in cash therefrom. The investigation authority arrested three foreign suspects who were still in Taiwan and retrieved TWD77.48 million that had been withdrawn. The three suspects were indicted and, based on the violation of Articles 359 and 339-2 of the Criminal Code, sentenced to four years and ten months, four years and eight months, and four years and six months, with criminal fines of TWD50,000, TWD40,000 and TWD30,000, respectively.

According to Article 45-1, paragraph 1 of the Banking Act, a bank shall establish an internal control system and audit system; regulations governing the objectives, principles, policies, operating procedures, qualifications and conditions for internal auditors, the scope of internal control audits that a certified public accountant shall be engaged to undertake and other matters requiring compliance shall be prescribed by the competent authority. Due to the security flaw that led to the above abnormal withdrawal activities, on 13 September 2016 the FSC fined First Commercial Bank TWD10 million for the violation of Article 45-1, paragraph 1 according to Article 129, sub-paragraph 7 of the Banking Act, and ordered the bank to suspend ATM cardless withdrawal temporarily in accordance with sub-paragraph 2, paragraph 1, Article 61-1 of the Banking Law; this facility was later resumed from 7 June 2017.

Far Eastern International Bank Data Breach

On 3 and 5 October 2017, malicious software was reported to be inserted into the system of Far Eastern International Bank, and USD60 million was transferred to accounts in Cambodia, Sri Lanka and the USA through the international SWIFT banking network. All but USD160,000 of the stolen funds was retrieved by the bank. The police in Sri Lanka have reportedly arrested two suspects.

On 12 December 2017, the FSC indicated that the bank's information security defence system was not completely sound, that the account management was inappropriate, that the bank had not strengthened its SWIFT safety system nor effectively conveyed the relevant rules and regulations to be complied with, and that the bank's internal control was not effectively implemented. Far Eastern International Bank

was fined TWD8 million for the violation of Article 45-1, paragraph 1 according to Article 129, subparagraph 7 of the Banking Act. The FSC also requested the bank to raise the expertise level of its information security unit, increase the number of members in its information security team, enhance its awareness of information security risk and strengthen the function of its information security system.

5.4 Due Diligence

In general legal due diligence, data protection compliance will be included in the overall legal compliance section, which focuses on whether the due diligence target has any judgment record or administrative punishment due to non-compliance issues, including non-compliance with data protection. The internal data protection rules and data protection compliance in respect of employment matters will be the focus of legal due diligence as well.

Furthermore, due diligence coverage and density in respect of data protection will be enlarged for certain types of industry. For example, if the target company's business is strongly involved in or related to personal data or information, such as a business related to targeted advertisements, the focus should be on whether/how the collection and processing of personal data comply with applicable laws. This may include but not be limited to the following:

- the type of data being collected and processed, and whether it includes any personal data or sensitive personal data;
- if yes, how the business collects, uses, shares, stores and deletes personal data;
- the lawful bases upon which the target company relies to collect and/or process personal data, and related supporting documents; and
- if the personal data is not collected directly from data subjects themselves, what contractual arrangements are in place with the collector of the data.

As for an industry that collects consumers' or customers' personal data for promotion or other purposes (eg, retailers or financial services providers), since the competent authorities of certain industries (eg, internet retailers, banks or finance industries) have enacted security regulations and maintenance plans for the protection of personal data files, besides the above-mentioned areas, the due diligence scope may also include whether proper security measures are implemented to prevent the personal data from being stolen or disclosed, and whether there is a security and maintenance plan in place for the protection of personal data files in accordance with the relevant regulations.

5.5 Public Disclosure

Under Taiwan law, a listing company shall disclose material information regarding the company on the website designated and maintained by the authority. "Material information" includes any material effect on company finances or business resulting from an administrative disposition, and the occurrence of any material event that results in circumstances where the administrative fines for one single event have accumulated to TWD1 million or more, or that causes a material loss to the company. Therefore, if administrative fines are imposed for one single event accumulating to TWD1 million or more due to violation of the Cyber Security Management Act (CSMA) (eg, failing to report knowledge of a cybersecurity incident to the central governmental authority), any cybersecurity incident causing material loss, or any of the administrative dispositions in accordance with the CSMA by the authority leading to a material effect on company finances or business, the listing company shall disclose such information. The disclosure shall include the information and content in the format required by the authority.

There are further disclosure requirements for certain specific industries, such as electronic payment enterprises, financial enterprises and travel agencies, which shall report cybersecurity or data breaches to the competent authority pursuant to the applicable laws and regulations within the time limit requested thereunder.

5.6 Other Significant Issues

There are no further significant issues.

Chen & Lin counts data protection as one of its main practice areas, due to the emerging technologies that are accumulating, compiling and analysing immense volumes of data. In total, the data protection group has 15 lawyers across two locations (Taipei and Hsinchu), who provide advice and assistance to clients from all over the world. The team combines legal experience and adaptability with advanced hi-tech skills and development. The firm is also well connected with law firms in other countries, and is able to provide an international service as a result of co-operation and co-ordination with those firms. Key practice areas are compliance, providing the latest regulatory developments, advising on appropriate measures for protecting an owner's data and not infringing another's right to data, reviewing and commenting on market practice relating to data protection, and handling dispute resolution, assisting clients to navigate investigations or court proceedings, to defend allegations of infringement, and to assert and enforce data protection regulations or contract arrangements.

AUTHORS

Che-Hung Chen is the partner in charge at Chen & Lin. His key practice areas are those relating to intellectual property, funding/capital and market behaviour and activities. Che-Hung Chen continues to practise in cases relating to data protection, and is currently handling a series of trade secret cases involving the protection of R&D data. Although there are limited professional bodies that relate to the practice of data protection law specifically, he is a frequent participant in activities relating thereto.

Doris Lu is a partner at Chen & Lin and is experienced in the practice areas of overseas and domestic IPO/SPO and fundraising, M&A transactions, inbound and outbound investment, financing, general corporate consultations and the drafting and negotiation of various contracts. She continuously and frequently provides data protection advice to various clients, most of which are multinational corporate clients and Taiwan listing companies.

Jakob Huang is a partner at Chen & Lin and practises in the areas of M&A, inbound and outbound investment, general corporate consultations, contractual business model design, and the drafting and negotiation of various contracts. He provides a data protection service to corporate clients in various fields of business, and provides data protection advice to e-commerce, video game and social media companies on their compliance with personal data protection regulation.

Ting-Yi Chen is an associate at Chen & Lin, whose key practice areas are intellectual property, corporate consultation and legal compliance. She has advised clients on data protection and privacy laws, and provided analysis of the resulting impact on data protection considerations from the perspective of Taiwan law for clients' issues. She continuously provides data protection services to various clients.

Chen & Lin

Bank Tower, 12th Floor
205 Tun Hwa North Road
Taipei
Taiwan (Republic of China), 105

Tel: +886 2 2715 0270
Fax: +886 2 2514 7510
Email: chchen@chenandlin.com
Web: www.chenandlin.com

宏鑑法律事務所
Chen & Lin Attorneys-at-Law