Chambers
AND PARTNERS

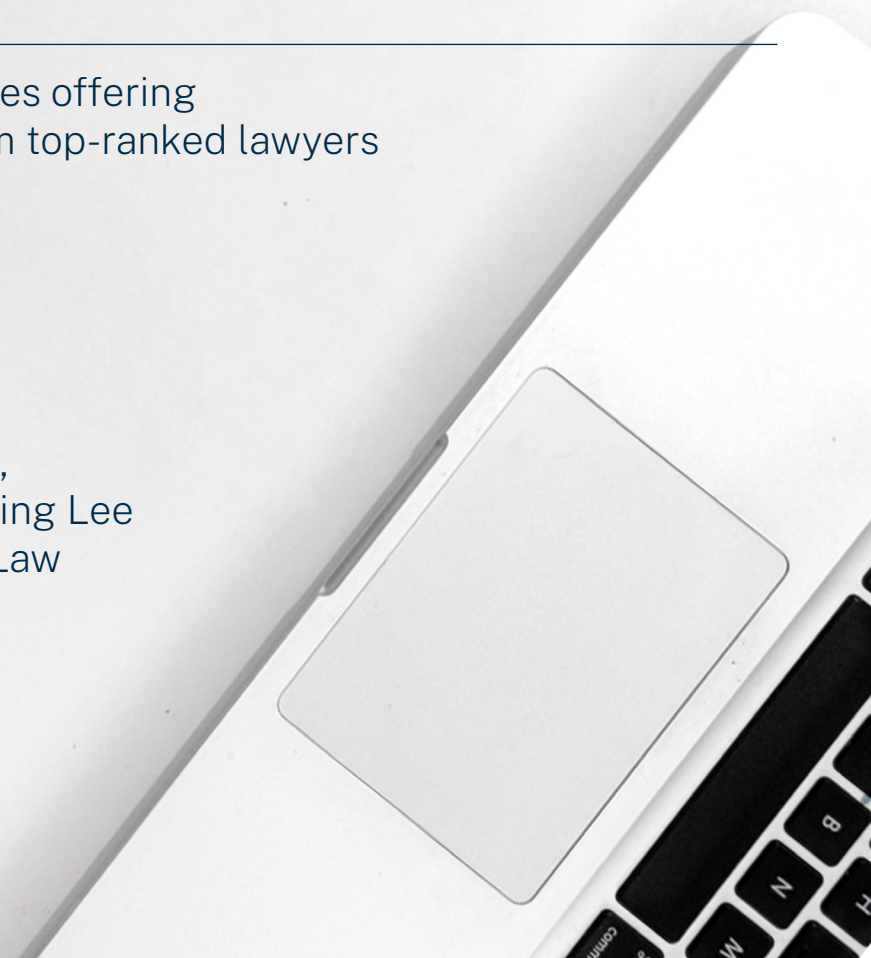
CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

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

Taiwan: Law & Practice

Che-Hung Chen, Doris Lu,
Jakob Huang and Meng-Ying Lee
Chen & Lin Attorneys-at-Law



TAIWAN

Law and Practice

Contributed by:
Che-Hung Chen, Doris Lu, Jakob Huang and Meng-Ying Lee
Chen & Lin Attorneys-at-Law

Contents

Chen & Lin Attorneys-at-Law 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 three locations (Taipei, Hsinchu and Kaohsiung), 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 include 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; handling dispute resolution; assisting clients in navigating investigations or court proceedings; defending allegations of infringement; and asserting and enforcing data protection regulations or contract arrangements.

Authors

Che-Hung Chen is the partner in charge at Chen & Lin. His key practice areas relate 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 frequently provides data protection advice and assists in project-type data protection compliance investigations for 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 games and social media companies on their compliance with personal data protection regulation.

Meng-Ying Lee is an associate at Chen & Lin, whose key practice areas are litigation, corporate consultation and legal compliance. She has advised clients on data protection and privacy laws and has provided analysis of the resulting impact on data protection considerations from the perspective of Taiwan law for clients' issues. She frequently provides data protection services, including compliance and project-type data protection compliance investigation, to various clients.

Chen & Lin Attorneys-at-Law

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: dorislu@chenandlin.com
Web: www.chenandlin.com

宏鑑法律事務所
Chen & Lin Attorneys-at-Law

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related 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 government agencies and certain private sectors. The PDPA has been effective since 1 October 2012 and regulates any person – including government 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, the criminal sanctions of the Criminal Code of the Republic of China may apply. If any national security issue is involved, the National Security Act may apply.

On 16 May 2023, the Legislative Yuan passed amendments to the PDPA to urge non-government agencies (ie, the private sector) to input manpower, techniques and funds for the purpose of fulfilling data protection obligations, and to provide support to relevant enforcement authorities for combating fraudsters. Two main points of the 2023 amendments are as follows:

- raising the administrative penalties imposed against non-government agencies for violating the obligation of security and maintenance measures; and
- designating the Personal Data Protection Commission (PDPC) as the dedicated competent authority of the PDPA (the Preparatory Office of the PDPC was formed on 5 December 2023, accordingly).

On 20 December 2024, the Preparatory Office of the PDPC announced a draft amendment to the PDPA. The public consultation period ended on 10 January 2025, during which opinions from various sectors were received. The main purpose of this amendment is to align with the establishment of the PDPC and to grant the PDPC relevant enforcement powers, including administrative supervision over both government and non-government agencies, as well as co-operation mechanisms with other competent authorities with regard to supervision on non-government agencies.

The main points of these amendments are as follows:

- the establishment of a supervision mechanism for government agencies;
- the requirement for government agencies or designated non-government agencies to:
  - (a) appoint a Personal Data Protection Officer responsible for promoting and overseeing personal data protection matters within the agency; and
  - (b) appoint auditor(s) responsible for planning and executing auditing activities

related to personal data protection management;
- the obligation for government agencies and non-government agencies to implement response measures, maintain records of incidents, and report personal data breaches, along with the revision of the conditions for notifying the affected parties; and
- procedures for selecting and evaluating high-risk industries and non-government agencies related to personal data breaches, with provisions for prioritising administrative inspections of these entities.

The 2024 draft amendments are still subject to review and discussion by the authorities. The PDPA currently in effect is the PDPA (2023 Amended). Therefore, unless otherwise referred to the draft amendments, the PDPA referred to hereunder will be the PDPA (2023 Amended).

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 recognised by APEC as the Accountability Agent for CBPR verification in Taiwan for domestic enterprises.

Taiwan also joined the EU-led Joint Declaration on Privacy and the Protection of Personal Data in October 2022. The declaration is intended to foster international co-operation to promote high data protection and privacy standards. Taiwan's inclusion will allow strengthening exchanges and co-operation with EU and Indo-Pacific countries.

Furthermore, in seeking 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 sub-national level are solely relevant to the implementation of those national laws and regulations by the different functioning bureaus of local government. Additionally, certain competent authorities have established specific regulations requiring security and maintenance plans for the protection of personal data within the industries under their supervision. These regulations are applicable to each specific industry.

1.2 Regulators

Since the amendments to the PDPA were passed, the PDPC will be the dedicated competent authority of the PDPA. Upon its official launch, the PDPC will integrate those enforcement powers and responsibilities (stated below) spread among the Ministry of Justice (MOJ), the National Development Council, central government authorities that supervise the business operation of non-government agencies, and

local government authorities. Further, the PDPC will prioritise the regulation of non-government agencies that do not have a clearly designated competent authority. As for non-government agencies that already have been governed by a competent authority due to the feature of business, transitional provisions will apply. During the transitional period, the supervision by their central or local competent authority will remain in effect temporarily, and the regulatory powers of each respective competent authority will be gradually migrated to the PDPC in phases. This approach aims to achieve the legislative policy goal of centralising and unifying personal data protection oversight.

Before the official launch of the PDPC (scheduled for August 2025), the relevant regulators and their authorities are as below.

The MOJ is the main regulator for personal data protection and is in charge of proposing the draft bill of the PDPA, and promulgating the Enforcement Rules of the PDPA (which will be migrated to the PDPC after it is official launched). The MOJ and the National Development Council are in charge of issuing various interpretations to answer questions in respect of compliance with the PDPA.

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

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

1.3 Enforcement Proceedings and Fines

Administrative Enforcement Proceedings

Under the PDPA, central and local government authorities have the power to conduct an audit and inspection on non-government agencies, for which they may access the premises of non-government agencies, request information, and copy and retain documents. If the non-government 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-government agency may raise an objection against such compulsory measures. However, if the government authority refuses to change such compulsory measures, the non-government 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 imposed penalties, and in respect of 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.

As noted in **1.2 Regulators**, the enforcement of the PDPA will be administered by the PDPC upon its official launch scheduled for August

2025. (The PDPC will prioritise the regulation of non-government agencies that do not have a clearly designated competent authority and gradually extend and include all other sectors whose data protection compliance is governed by competent business authorities). Nevertheless, the enforcement of the PDPA is currently still administered by central relevant business government authorities and local government authorities, rather than by any single government authority. For current circumstances, it is difficult to obtain a full picture in respect of the enforcement status of different central and local government 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 whether 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), the competent authority of financial institutions, will be relatively aggressive compared to other government authorities.

Calculation of Administrative Fines

Fines for violations of the PDPA range from TWD20,000 to TWD15 million. There are no further explicit unified standards for penalties regarding violation of the PDPA. Nevertheless, as a general rule for administrative control, the fines imposed by administrative authorities shall be in proportion to the degree of violation, and must not involve abuse of discretion or violate the principle of proportionality. The authorities may consider factors such as the circumstances of the violation and frequency of violations when determining the amount of the fine.

1.4 Data Protection Fines in Practice

Heaviest Penalty

The FSC's heaviest penalty ever imposed for a bank's personal data breach was in 2023.

In September 2022, the FSC received an anonymous tip-off alleging a cybersecurity breach at Shanghai Commercial & Savings Bank, Ltd, which led to the leakage of customer personal data. After an investigation, it was confirmed that the bank had leaked the names and ID card information of 14,000 customers. In November 2023, the FSC imposed a fine of TWD10 million on Shanghai Bank, marking the heaviest penalty ever imposed by the FSC for a bank's personal data breach that year. According to the FSC, the following deficiencies were found in the bank's customer data confidentiality and information security system, both in terms of internal control and operational aspects.

- Failure to establish a comprehensive internal control system.
  - (a) Failure to establish appropriate personal computer administrator rights regulations – the bank only clarified the policy on changing the personal computer administrator password every six months on 15 December 2022, after the incident. Prior to this, password changes were not regularly implemented, which exposed customer data to the risk of leakage.
  - (b) Failure to establish comprehensive portable device management regulations – personnel authorised to use portable devices were still able to take internal data offsite, and there were no appropriate access controls in place for reading the data, which undermines information security protection.
- Failure to properly execute the internal control system.

(a) Failure to record personal data usage – the bank's personal data security maintenance guidelines require recording the use of personal data, retaining trace data, or relevant evidence. However, the report system did not retain personal data usage traces in accordance with internal regulations, which hinders the ability to track the usage of personal data in the event of a data breach and affects the auditing timeline.
(b) Failure to confirm the implementation of system security updates – the bank's information equipment authorisation and protection management rules, as well as the personal computer usage management regulations, stipulate that operational environment changes should undergo proper testing, and security updates delivered to workstations should be confirmed. However, prior to and during system updates, the bank failed to identify vulnerabilities in the security monitoring software and confirm its execution on workstations. As a result, the software failed to start normally, preventing proper control and recording of portable device data access, which affected audit effectiveness and made it impossible to assess actual damage, hindering subsequent investigation procedures.

Vehicle-Sharing Platform Risks Exposure of Personal Data of More Than 400,000 of its Users

In January 2023, a security researcher discovered a database containing iRent (a large vehicle-sharing platform in Taiwan) customers' personal data (including full names, cell phone numbers, email addresses, home addresses, photos of their drivers' licences, and partially redacted payment card details) on a cloud server that was inadvertently accessible to the public. Because the database was not password-protected or encrypted, anyone on the internet could access this iRent customer data. The database, which contained about 4.2 terabytes of data, was exposed on the open web for at least nine months before the researcher discovered it.

This incident instantly captured widespread public attention as iRent is the largest vehicle-sharing platform in Taiwan. iRent explained that its temporary database did not properly block external connections, resulting in the database potentially being accessed by external parties using specific tools and techniques to access information of members, with 400,000 members potentially being affected.

The Directorate General of Highways and the Taipei Municipal Transportation Bureau separately imposed a fine of TWD200,000 and TWD90,000 for the data leakage. iRent was also ordered to improve its data security.

After this incident, a councillor of Taipei City Council considered that because the amount of fines under Taipei City's autonomous ordinance for data breach was too low, enterprises often overlooked the severity of such incidents and did not give earnest attention to data security measures. With fines set at a level that does not proportionately reflect the potential impact and damages resulting from breaches, there is a diminished incentive for enterprises to proactively invest in robust security measures. Therefore, the councillor proposed a draft amendment to the "Taipei City Autonomous Ordinance Governing Ridesharing Services Management". This amendment was passed in December 2023. Under the new ordinance, if a data breach results from the enterprise's intentional act or

negligence, the Department of Transportation of Taipei City may revoke or cancel its operational licence.

1.5 AI Regulation

In Taiwan, the PDPA establishes a comprehensive legal framework governing the collection, processing and use of personal data. This framework is designed to capture a wide range of activities related to personal data, ensuring that regulations are applicable regardless of the specific methods employed or the distinct purposes for which the data is collected or used. The PDPA provides a general set of guidelines that can address the dynamic and evolving nature of data-related practices. In other words, data protection in the context of the use of AI systems is also the targeted scope governed by the PDPA.

Taiwan's government also acknowledges the rapid development of emerging technologies, such as AI, and the complex data-related challenges these innovations bring. As a result, the government is also continuously revisiting and examining whether the current regulatory regime could duly catch all new relevant technologies. As such, in addition to the PDPA as the primary law of data protection, several draft regulations governing AI have been proposed and are presently under discussion, in which several requirements and mechanisms for extending the protection of personal data are outlined:

- data minimisation;
- data protection by design and by default;
- personal data de-identification; and
- providing personal data in a commonly used format.

1.6 Interplay Between AI and Data Protection Regulations

The interplay between data protection laws reflects a layered approach, where the PDPA serves as the overarching framework, providing general principles and rules for the processing of personal data. However, as new technologies and practices emerge, other laws and regulations tailored to specific sectors or issues – such as those governing AI – can impose additional requirements that complement, supplement or refine the general provisions of the PDPA.

The new draft AI regulations introduce additional, specific data protection requirements that were not explicitly covered under the existing PDPA (ie, requirement of data minimisation, data protection by design and by default, de-identification and ensuring data portability). The relationship between these evolving regulations and the PDPA highlights the dynamic nature of data protection laws, as regulators aim to address emerging challenges driven by technological advancements. Additionally, competent authorities, such as the Ministry of Digital Affairs, have issued guidelines for privacy-enhancing practices to help businesses navigate the use of new technologies while simultaneously ensuring robust data protection. To ensure comprehensive compliance, businesses will need to navigate both the existing PDPA framework and the new draft regulations, while staying prepared for future updates to the legal landscape.

2. Privacy Litigation

2.1 General Overview

Trends in Data Breach Litigation Related to Fraudsters Exploiting Leaked Personal Data

In Taiwan, cases of fraudsters exploiting leaked personal data to scam data subjects have

become increasingly prevalent. There is a growing trend of data subjects, who suffer both pecuniary and non-pecuniary damage, seeking compensation from the businesses responsible for the data breaches. The majority of courts held that the pecuniary damage suffered by the data subjects is a result of the fraudsters' actions, not those of the business, and therefore, no causation exists between the data breach and the pecuniary damage. However, some of them further held that the emotional distress suffered by the data subjects in the fraud event is linked to the business's data breach, allowing data subjects to seek compensation for non-pecuniary damage.

Overview of the Impact of Supranational/International Developments on Domestic Litigation

Taiwan courts apply the "reasonable expectation of privacy" standard originating from US law in privacy litigation

Privacy rights are distinguished into two types: "freedom from intrusion into personal private life" and "the right to control personal data (ie, information privacy)". According to decisions made by the Constitution Court, individuals are still protected by these freedoms even in public spaces, though their claim to "freedom from intrusion" is limited to situations where they have a reasonable expectation of privacy from others. Therefore, whether an individual has the "freedom from intrusion" in public spaces is assessed based on the "reasonable expectation of privacy" standard, which originates from US law and is adopted and considered by the Taiwan court in privacy infringement cases.

For example, in a case regarding violating parking rules, the key evidence is the record of the informant's driving recorder recording the parking violation behaviour and the car information of the claimant, and the claimant arguing such record infringed his privacy. The court adopted a "reasonable expectation of privacy" standard to determine whether a privacy infringement existed. It provided that if data subjects drive their own vehicles in a public place, they are clearly disclosing their vehicles' licence plate numbers to the general public, and the data subjects should be aware that the licence plate numbers can be easily linked to the vehicle owners, thus revealing their movements. Therefore, the data subjects do not have a subjective expectation of privacy regarding the licence plate numbers or brief driving movements. However, if the recording was specifically used to monitor and record a specific individual's movements for an extended period of time, the data subjects would still have a subjective expectation of privacy regarding their personal whereabouts. Nevertheless, even if the data subjects may hold a subjective expectation of privacy concerning their licence plate number or brief movements, as this personal data can be observed by the public with the naked eye and without the use of any technology, it is difficult to consider such an expectation as objectively reasonable. It is clear that the court assesses privacy infringement by reference to the "reasonable expectation of privacy" standard.

Right to be forgotten

The "right to be forgotten", as established by the European Court of Justice, has also been invoked by parties in Taiwan's courts. (see **2.2 Recent Case Law** for details).

2.2 Recent Case Law

Case Regarding Right to be Forgotten

A well-known case is one in which a former professional baseball CEO claimed the right to be forgotten and requested Google Inc. to remove search results related to his match-fixing scan-

dal. This case began in 2017, and has been heard by the district court, the High Court and the Supreme Court. The Supreme Court has twice remanded the case for re-examination by the High Court. In these judgments, the courts generally recognise that the right to be forgotten falls within the scope of privacy rights and is protected under the Constitution. However, search engine operators' provision of search results, although commercially driven or for profit, should still be protected under the freedom of speech protected by the Constitution. Such search results should not be arbitrarily restricted or deleted, as doing so would undermine the performance freedom and neutrality of search engine operators which could, in turn, affect the public's perception and judgement, and even threaten the foundation of democratic constitutionalism. Therefore, when determining whether certain search results should be deleted, courts seek to strike a balance between public interest and privacy rights. The Supreme Court re-stated the foregoing view and opined that the data subject may also request the deletion of the collected or processed data if there is a more significant interest that needs to be protected. This includes many factors such as whether the data subject is a public figure, and whether the data has been outdated or causes disproportionate negative privacy impacts on the data subject. The Supreme Court also considers whether the deletion would affect or hinder the public's right to know.

From the above, it is clear that the courts attempt to balance public interest with privacy rights. In deciding whether specific search results should be deleted, the High Court and the Supreme Court have reached different conclusions based on the consideration of those factors. The match-fixing scandal was 14 years ago. At the second review of the Supreme Court in 2024, it dismissed the judgment of the High Court again and requested the High Court to re-consider and seek a balance between the right to be forgotten and the public's right to know based on all the relevant factors.

2.3 Collective Redress Mechanisms

Collective Redress Mechanisms – Class Action

The PDPA provides a collective redress mechanism through class actions for data protection violations. 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 in its own name.

The First Data Breach Class Action

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.

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services

3.1 Objectives and Scope of Data Regulation

Regulations Applicable to IoT Services

Currently, there is no specific legislation that directly governs IoT services with regard to data protection. However, IOT services frequently involve the collection, processing and transmission of significant volumes of personal data. As such, the use of IOT services in relation to data protection should be subject to the general provisions and principles outlined in applicable data protection laws, such as the PDPA. Consequently, in the absence of dedicated IoT regulations, the overarching framework provided by the PDPA applies to IoT service providers handling personal data.

The Rights and Obligations of Data Holders and Data Processing Services

Under the PDPA, any collection, processing and use of personal data is governed by its provisions. The PDPA does not introduce a specific distinction between "data controllers" (or data holders) and "data processors" (data processing services). While many data protection frameworks, such as the GDPR, explicitly define these roles, the PDPA focuses primarily on the responsibilities of entities involved in data collection, processing and use without separately categorising them. Instead, it sets forth general obligations for all parties involved in the handling of personal data, irrespective of the role the entity plays in the data processing chain.

Under the PDPA, the collection, processing and use of personal data shall comply with essential requirements. These requirements include the following.

- Informing the data subject: Businesses must provide information to the data subject regarding the collection, use and processing of their personal data. This includes informing them about the specific items outlined under the PDPA, such as the purposes of data collection, the categories of data being collected, the retention periods, and the rights of the data subject to access, correct and delete their data.
- Data subject's consent or other lawful requirement: The collection, use and processing of personal data must be based on the data subject's consent or any other lawful requirements. In cases where consent is not required, data processing may be lawful under other circumstances such as when it is expressly required by law, or there is a contractual or quasi-contractual relationship between the businesses and the data subject, and proper security measures have been adopted to ensure the security of the personal data.
- Purpose limitation: Personal data must only be used for the specific purposes that were initially communicated to the data subject at the time of collection. This principle ensures

that individuals' personal data is not misused for other purposes without their knowledge. If data is to be used for a purpose outside the initially stated purpose, it must be based on a clear lawful requirement. Such lawful grounds may include instances where the use is expressly required by law, when it is necessary for protecting public interests, or where it is to prevent harm to the life, body, freedom or property of the data subject.
- International transfer: In principle, international transfer of personal data is allowed under the PDPA. However, certain competent authorities may impose restrictions or prohibit businesses from transferring personal data to specific jurisdictions under certain circumstances – eg, where the level of protection for personal data does not meet the required standards.
- Security measures: Businesses are required to implement appropriate technical and organisational security measures to protect personal data from risks such as unauthorised access, theft, alteration, loss or destruction. These security measures must be tailored to the nature of the data being processed and the risks involved, and must be regularly reviewed and updated to address emerging threats. It is also required to ensure that any commissioned third parties involved in processing personal data adhere to the appropriate security standards.

3.2 Interaction of Data Regulation and Data Protection

Since Taiwan follows the civil law system, data protection requirements are primarily governed by the relevant data protection regulations, with the PDPA being the key piece of legislation. In addition to the PDPA, sector-specific laws may apply when it comes to certain data protection requirements in specific industries. For example, the Banking Act sets forth additional data protection provisions for the banking sector.

3.3 Rights and Obligations Under Applicable Data Regulation

Please see **3.1 Objectives and Scope of Data Regulation** for details.

3.4 Regulators and Enforcement

The current enforcement of the PDPA is administered by the central government authorities that supervise the business operation of non-government agencies and local government authorities. As stated in **1.2 Regulators**, upon its official launch (scheduled for August 2025), the PDPC will integrate the enforcement powers and responsibilities spread among the MOJ, the National Development Council, central government authorities that supervise the business operation of non-government agencies and local government authorities (the PDPC will prioritise the regulation of non-government agencies that do not have a clearly designated competent authority, and gradually expand the scope to all other industry).

4. Sectoral Issues

4.1 Use of Cookies

The PDPA does not have specific provisions directly addressing cookies. Nevertheless, their use, which typically involves collecting personal data from users' devices, must comply with the general principles of the PDPA. This includes:

- providing certain information required by the PDPA (businesses must provide clear information in respect of certain items prescribed under the PDPA, such as the name of the business, the types of personal data being collected, the rights of the data subjects, and

the duration, location, recipients and methods of data use; this information is usually provided in the form of a cookie, policy or privacy notice);
- obtaining informed consent from data subjects (businesses must obtain informed consent from users before placing cookies on their devices);
- ensuring that data is used only for specified purposes within the scope of data subjects' consent (businesses cannot use cookies for unrelated or secondary purposes without obtaining further consent from users);
- implementing appropriate security measures to protect personal data (businesses must implement appropriate technical and organisational measures to protect personal data collected through cookies from unauthorised access, disclosure, alteration or destruction); and
- respecting data subjects' rights, such as to access, rectify, delete, or request a copy of their personal data, or demand the cessation of the collection, processing or use of their personal data.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised Advertising

Personalised advertising is not specifically regulated under a separate legal framework in Taiwan, but it is governed by the general provisions of the PDPA. Since personalised advertising often involves the collection and analysis of personal data to target individuals with tailored ads by way of collecting and analysing the browser records and footprint and at least partial IP information, it must comply with the requirements set out in the PDPA (please refer to **4.1 Use of Cookies**). Therefore, businesses engaging in personalised advertising must adhere to the PDPA's general data protection principles to ensure legal compliance.

Other Online Marketing Practices

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 must stop immediately. Also, the non-governmental agency should offer ways for the data subject to express their refusal at the time such marketing first appears in public, and should compensate any necessary cost and expense for expressing such refusal.

Moreover, the Financial Holding Company Act provides that financial holding companies' subsidiaries engaging in co-selling activities among themselves should apply to the FSC for prior approval and ensure that such activities will not harm the interests of customers. The subsidiaries of the financial holding company should 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.

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

4.3 Employment Privacy Law

In Taiwan, the PDPA plays a primary role in shaping data protection with respect to the employment relationship. Employers must comply with the general requirements of the PDPA when col-

lecting, processing, and using employees' personal data, such as obtaining employee consent for data collection and adhering to purpose limitations.

Besides general requirements, issues relevant to workplace privacy mainly focus on email monitoring and whistle-blowing.

Email Monitoring

In most cases, a 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 will be monitored, or if the employees have signed written consent for email monitoring, it is hard to say that the employees have a reasonable expectation of privacy for such emails.

Whistle-Blowing

Private sector

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 should keep the identity of the complainant in confidence, and should 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.

Public sector

On 27 December 2024, the Public Interest Whistle-Blower Protection Act was passed by the Legislative Yuan. The scope of this Act and the agencies responsible for handling whistle-blowing apply to the public sector, state-owned enterprises, and government-controlled businesses, but do not extend to the private sector. Further, the Act defines a whistle-blower as a public servant or personnel working in a government agency, as well as employees working in state-owned enterprises or government-controlled businesses.

Whistle-blowers must file a report with the appropriate agency under their real name. If they do not receive notification of the acceptance and

investigation of their report within 20 days, they may urge the agency to take action.

To protect whistle-blowers from retaliation and harm to their rights due to their whistle-blowing actions, the Act explicitly prohibits taking adverse actions against whistle-blowers for their reporting, including dismissal, removal from position, deprivation of benefits related to promotion, and unfavourable changes to their work location, job responsibilities, etc. Further, anyone who discloses a whistle-blower's identity without justification may be sentenced to imprisonment and may also be fined.

4.4 Transfer of Personal Data in Asset Deals

In asset deals involving the transfer of personal data, if the privacy notice provided by the original data collector adequately covers the transferee as a potential data processor or user and has been consented to by a data subject, it is not mandatory under Taiwanese law for the transferee to issue a separate notice to the data subject and obtain a new consent upon processing or using the data.

However, if the transferee is not explicitly included in the scope of potential processors or users in the original privacy notice to be consented to by the data subject, the transferee is obligated to inform the data subject and provide a new privacy notice before processing or using the data. The notice shall include, among others, the name of the transferee, the purpose of the collection, the retention period, the data subjects' rights and the source of the data. Additionally, in practice, the data subject will be given opt-in/opt-out options upon receiving such notice from the transferee.

5. International Considerations

5.1 Restrictions on International Data Transfers

Under the PDPA, in general international data transfer is permitted, while the government authority in charge of the pertinent industry may, at its reasonable discretion, impose limitations on international data transfers if:

- they involve important national interests;
- a national treaty or agreement specifies otherwise;
- the country receiving the 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.

Pursuant to the above provision and relevant laws governing particular industries, certain authorities further promulgate and require certain data residency/data localisation requirements whose nature will impose certain restrictions on international data transfer. For example, the FSC promulgates certain data residency requirements for financial institutions.

In addition, certain authorities promulgate and impose restrictions in terms of which certain specific industries are prohibited from transferring data to a specific territory. For example, communications enterprises, social worker offices or human resource agencies are prohibited by respective governmental authorities in charge of the pertinent industry from transferring their subscribers' or their clients' personal data to China.

5.2 Government Notifications and Approvals

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

Further, electronic payment businesses wishing to outsource their data-processing operations should obtain the FSC's approval in advance.

5.3 Data Localisation Requirements

As stated in **5.1 Restrictions on International Data Transfers**, international data transfers are in general permitted by the PDPA, while it leaves the room and flexibility to the relevant competent authority to impose restrictions at its discretion based on the regulation and management needs of the specific industry. Therefore, the relevant competent authority may still promulgate sector-specific rules governing data localisation for a specific industry. Please see **5.1 Restrictions on International Data Transfers** and **5.2 Government Notifications and Approvals** for details.

5.4 Blocking Statutes

There is no concept of "blocking" in Taiwan.

5.5 Recent Developments

The general rules and handling in relation to the international transfers of personal data are set out in **5.1 Restrictions on International Data Transfers** to **5.3 Data Localisation Requirements**. With respect to a new development on 18 December 2024, Taiwan Food and Drug Administration, the Ministry of Health and Welfare, announced a draft to "restrict the international transfer of personal data by the wholesale and retail pharmaceutical industry to China, Hong Kong, and Macau". In this draft, it is stipulated that the wholesale and retail pharmaceutical industry shall not transfer the personal data it collects, processes and uses to China, Hong Kong and Macau unless an exception applies. The exceptions include, among others:

- where the personal data cannot be identified, either directly or indirectly;
- where the personal data is not obtained in connection with pharmaceutical-related business activities;
- where the personal data belongs to an employee of the wholesale and retail pharmaceutical industry, or personal data is related to service providers or business partners and is obtained by pharmaceutical wholesalers or retailers during the course of their business operations; and
- where the headquarters or parent companies of the wholesaler or the retailer have obtained or comply with certain certification, such as an adequacy decision under the GDPR.

The draft regulation is open for public comment and the consultation period ends in mid-January 2025. The regulation is expected to be officially announced in June 2025.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com