IN-DEPTH

Privacy, Data Protection And Cybersecurity

TAIWAN

LEXOLOGY

Privacy, Data Protection and Cybersecurity

EDITION 12

Contributing Editor

David C Lashway

Sidley Austin LLP

In-Depth: Privacy, Data Protection and Cybersecurity (formerly The Privacy, Data Protection and Cybersecurity Law Review) provides an incisive global overview of the legal and regulatory regimes governing data privacy and security. With a focus on recent developments, it covers key areas such as data processors' obligations; data subject rights; data transfers and localisation; best practices for minimising cyber risk; public and private enforcement; and an outlook for future developments.

Generated: November 20, 2025

Taiwan

Jaclyn Tsai, **Jaime Cheng** and **Hannah Kuo**
Lee Tsai & Partners

Summary

Introduction

Primary legislation

Taiwan takes an omnibus approach to the protection of personal data. The Computer-Processed Personal Data Protection Act (CPDPA) was promulgated in 1995, which regulated the computer processing of personal data by governmental and non-governmental entities. In 2004, the grand justices held in Judicial Yuan Grand Justice Judicial Interpretation No. 585 that the right to privacy is a necessary fundamental right to human dignity, individual subjectivity and personality development and thus is a constitutional right. In 2005, the grand justices further held in Judicial Interpretation No. 603 that the government may collect people's private information (e.g., fingerprints) only when:

1. such collection is in consideration of a specific significant public interest;
2. the purpose of such collection is specified by law;
3. such collection is necessary and closely related to the achievement of a significant public interest; and
4. the use of such information shall not exceed the scope of the statutory purpose.

Consistent with these interpretations, the CPDPA was then amended and renamed the Personal Data Protection Act (PDPA) in 2010 and, along with its related enforcement rules, became effective on 1 October 2012. Under the PDPA, the scope of regulation is no longer limited to computerised processing of personal data information but applies to all entities (government and non-government, foreign and domestic entities) that collect, process or use personal data within the territory of Taiwan. Moreover, the PDPA limits the disclosure of personal data to specific circumstances, such as responding to government requests to the extent that a disclosure procedure meets the applicable requirements and the use of such data does not exceed the scope of the purpose. In addition to the PDPA, central competent authorities of industries have also promulgated additional regulations for implementing and interpreting the PDPA.

As for cybersecurity, the Cyber Security Management Act (CSMA) serves as a standard for cybersecurity plans. The National Communications Commission (NCC) provides the regulations governing the security of personal data collected by telecom enterprises in the telecommunications industry. According to the CSMA, the competent industrial authorities may also require non-governmental agencies to implement cybersecurity protection plans.

In terms of the restrictions on government surveillance, the Communication Security and Surveillance Act (CSSA) defines the scope of government surveillance powers and the procedural requirements.

Regulatory authorities

The PDPA was amended on 31 May 2023. The amendment includes the establishment of a single competent authority (i.e., the Personal Data Protection Commission (PDPC)), which

will replace the role of the National Development Council (NDC), industry authorities and the municipality, city or county governments concerned. The PDPC shall be established in accordance with a judgment of the Constitutional Court. In the meantime, the preparatory office of the PDPC was established on 5 December 2023 to replace the role of the NDC and is responsible for the establishment of the PDPC and further amendment of the PDPA.

Privacy advocates

The two main advocates of the right to privacy in Taiwan are:

1. the Data Protection Association of the Republic of China, a non-governmental organisation that promotes personal data privacy, development and improvement of data security technology, and data security services; and
2. the Taiwan Association for Human Rights, a non-governmental organisation that focuses on issues related to human rights, including privacy rights, and promotes personal data protection through monitory regulatory developments, commenting on proposed legislation and advocacy.

Integration with international standards

As a member of the Asia-Pacific Economic Cooperation (APEC), Taiwan has joined the APEC cross-border privacy rules (CBPR) system. On 21 April 2022, Taiwan, the United States, Canada, Japan, South Korea, Singapore and the Philippines, as the founding members, officially announced the establishment of the Global Cross-Broder Privacy Rules Forum (Global CBPR Forum) to promote information exchange and personal data protection.

Year in review

In response to the Constitutional Court's 2022 decision (111-Xian-Pan-Zi No.13), which held that the lack of an independent personal data supervisory mechanism was unconstitutional, the PDPA was amended on 31 May 2023. The amendment provides for the establishment of the PDPC, which will assume responsibilities previously exercised by the NDC and other authorities. A preparatory office was launched on 5 December 2023 to facilitate the transition.

To implement the PDPC, the Executive Yuan released the draft Organizational Act of the PDPC and a draft amendment to the PDPA on 27 March 2025, designating the PDPC as an independent authority with a collegial decision-making structure. Commissioners are guaranteed tenure to ensure institutional independence.

The draft amendment to the PDPA grants the PDPC powers such as centralised receipt of data breach notifications. It also requires each government agency to appoint a chief data protection officer and mandates that private entities comply with security measures set by the PDPC. To enable a smooth transition, certain non-governmental agencies may

remain under their current supervisory framework for up to six years as the PDPC gradually assumes full oversight.

Regulatory framework

Privacy and data protection legislation and standards

The PDPA defines personal data as 'a natural person's name, date of birth, national ID number, passport number, specific features, fingerprints, marital status, family information, education, employment, medical records, medical procedures, genetic information, sexual life, health examination information, criminal history, contact information, financial situation, social activities, and any other information that could be used directly or indirectly to identify an individual.'

Medical records, genetic information, sexual life, health examinations, and criminal records are sensitive personal data that may not be collected, processed, or used without legal cause.

The scope of the PDPA covers government agencies and non-government agencies (i.e., natural persons, legal persons, or other groups)[1] with varying requirements on their collection, processing and use of personal data.

General obligations for data handlers

The general principles underlying the PDPA on the collection, processing, and use of personal data are that the foregoing activities shall be carried out in a way that respects the data subject's rights and interests, in an honest and good faith manner, shall not exceed the necessary scope of the specified purposes and shall have legitimate and reasonable connections with the purposes of collection.[2]

Prior to collecting personal data, government and non-government agencies shall inform the data subject of:

1. the name of the agency;
2. the purpose of the data collection;
3. the type of personal data they aim to collect;
4. the time frame, territory, recipients, and method of use;
5. the rights under Article 3 of the PDPA and the methods for exercising such rights;
6. for information provided directly by the data subject, data subjects' rights and interests that will be affected if they elect not to provide their personal data; and
7. for information not provided by the data subject, the source of personal data.

For a government agency to collect or process personal data, it must have a specific purpose, and it must be on one of the following bases: the personal data collected is within the scope necessary for the said government agency to perform its statutory duties, the

data subject's consent has been obtained, or the rights and interests of the data subject will not be infringed.[3]

For non-government agencies to collect or process personal data, it must have a specific purpose and have one of the following bases:

1. express stipulation by law;
2. a contractual or similar relationship with the data subject where proper security measures have been adopted to ensure the security of the personal data;
3. the personal data was freely disclosed by the data subject or other entity legally permitted to disclose the personal data;
4. academic institutions must conduct statistical or academic research that benefits the public, and the personal data is processed by the provider or disclosed by the data collector in a way that may not directly identify the data subject;
5. consent of the data subject is obtained;
6. it is necessary for the public interest;
7. the personal data is obtained from publicly available sources unless the data subject prohibits the processing and use of such data, and he or she has an overriding interest; and
8. the rights and interests of the data subject will not be infringed.[4]

Furthermore, government agencies shall appoint dedicated personnel to implement security and maintenance measures, and non-government agencies shall implement proper security measures to prevent personal data from being stolen, altered, damaged, destroyed, or disclosed.[5] The industry authorities may further designate and order certain non-government agencies to establish a security and maintenance plan to protect personal data files and a guideline on disposing of personal data following a business termination.-[6]

Data subject rights

Data subjects have the following rights with respect to their personal data, and these rights may not be waived or restricted by contract:

1. the right to inquire about and review their personal data;
2. the right to request a duplicated copy of their personal data;
3. the right to supplement or correct their personal data;
4. the right to discontinue collection, processing and use of their personal data; and
5. the right to request the deletion of their personal data.[7]

If a government or non-government agency violates the PDPA in collecting, processing, or using personal data, data subjects may request the deletion of their personal data and for the agency to stop processing and using their personal data.[8]

Specific regulatory areas

Aside from the PDPA, there are other regulations governing personal data in other fields. For example, the Employment Services Act (ESA) states that employers may not request job seekers or employees to surrender private information irrelevant to employment.[9] In the medical field, all citizens are insured through national health insurance, and the use of personal data collected and stored on national health insurance cards is governed by the Regulations Governing the Production and Issuance of the National Health Insurance IC Card and Data Storage.

Technological innovation

In recent years, the government has been developing regulations and pilot plans for technology industries, including those involving personal data and cybersecurity, such as the following:

1. in September 2019, the Ministry of Science and Technology (which reorganised as the National Science and Technology Council in July 2022) established the AI Technology R&D Guidelines for technological researchers, which requires artificial intelligence (AI) researchers to adhere to relevant regulations on the collection, processing, and use of personal data and implement appropriate safeguards for data storage in AI systems to protect the dignity and rights of individuals; and
2. the Unmanned Vehicles Technology Innovative Experimentation Act, announced on 19 December 2018, requires participants in the regulatory sandbox to adopt appropriate and sufficient data security measures during the period of innovative experimentation to ensure the security of data collection, processing, utilisation and transmission, and to comply with the provisions of the PDPA.

International data transfer and data localisation

As mentioned above, Taiwan is a member of APEC, and Taiwan officially became a member of the CBPR system on 23 November 2018. Under this system, a total of 15 personal data-competent authorities from Taiwan joined the APEC Cross-Border Privacy Enforcement Arrangement (CPEA),[10] strengthening information sharing and cooperation in privacy investigations and enforcement with other member institutions. Furthermore, in June 2021, Taiwan's Institute for Information Industry formally became an accountability agent for the CBPR and will assist and certify that domestic companies implement their privacy policies and practices in compliance with the requirements under the CBPR system.

The PDPA does not restrict the cross-border transfer of personal data unless otherwise restricted by the central competent authorities. According to the PDPA, central competent authorities may impose restrictions on the cross-border transfer of personal data in the following cases:

1. when it involves major national interests;
2. when an international treaty or agreement so stipulates;

3. when the receiving nation lacks adequate regulations on personal data protection that may harm the rights and interests of the data subjects; or
4. when the transfer of personal data to a third country (region) is to circumvent the PDPA.

To date, only three cross-border restrictions have been imposed by the industry authorities. The first was made by the NCC on 25 September 2012, prohibiting communications enterprises from transmitting their clients' personal data to mainland China. The second was made by the Ministry of Health and Welfare on 21 January 2022, prohibiting social worker offices from transferring their clients' personal data to the territory of Mainland China. The third was made by the Ministry of Labour on 20 February 2023, prohibiting human resources recruitment industry from transferring personal data to the territory of Mainland China. All of these restrictions are still effective as of the time of writing.

To strengthen administrative supervision, the central competent authority or local governments may authorise investigators to inspect non-governmental entities when they deem it necessary to supervise international information transmission or suspect illegal activities.

Company policies and practices

Fifty-nine industries have been designated by industry authorities to set up a security and maintenance plan for the protection of personal data files, including the financial industry, the telecommunications industry and the human resources agency industry. For example, companies in the financial industry[11] and the telecommunications industry[12] are required to adhere to the following regulatory measures:

1. establish and implement a safety precaution plan for protecting personal data;[13]
2. establish a procedure for managing personal data;[14]
3. establish emergency measures to protect personal data in the case of safety threatening incidents;[15] and
4. establish a procedure for storing relevant records and evidence.[16]

Organisations in other industries are required to implement similar regulatory measures as stated above.

In addition, the Copyright Collective Management Organization manages the economic rights on behalf of multiple economic rights holders and will collect and use the holder's personal data. The Ministry of Economic Affairs has accordingly set up a security and maintenance plan and required the Copyright Collective Management Organization to not only implement similar regulatory measures as stated above but to also review the personal data managed by the Copyright Collective Management Organization and create a personal data list.[17]

Collection and use of employee and potential employee information

An organisation's collection of personal data from employees or potential employees should adhere to the PDPA and the ESA and its enforcement rules. As a general principle, employers shall respect the rights of employees and potential employees and refrain from overstepping the scope necessary for economic demands or public interest and limit the use of such data in a manner reasonably relevant to the organisation's goal.[18] For example, under the ESA, when an organisation needs to conduct background checks of applicants for potential employment, the organisation may not request private information that is irrelevant to the purpose of employment or withhold applicants' identification cards, work certificates, or any other certifying documents without the employee's consent.[19]

Discovery and disclosure

Entities disclosing personal data at the request of the government should still follow the PDPA

Non-government agencies providing personal data at the request of government agencies constitutes the use of personal data for a purpose other than the purpose the data was collected for, as stipulated in the PDPA, in which case, the use is limited to the following circumstances:

1. it is explicitly allowed by the law;
2. it is necessary for the public interest;
3. it is to prevent harm to a data subject's life, body, freedom, or property;
4. it is to prevent significant harm to the rights and interests of others;
5. government agencies and academic institutions must conduct statistical and academic research that benefits the public, and the personal data is processed by the provider or disclosed by the data collector in a way that may not directly identify the data subject;
6. the consent of the data subject is obtained; and
7. it is in the interest of the data subject.

Presentation of civil litigation documentary evidence

Taiwan does not have a discovery procedure in civil litigation. Relevant documents identified as documentary evidence should be produced by the parties involved,[20] or a party may request the court to order the opposing party or a third party to produce such documents.[21]

If the contents of the documents a party is obligated to produce include privacy or trade secrets of the party or a third party where the disclosure of which may cause significant harm, the party may refuse to produce such content. To determine whether the party has a justifiable reason to refuse the production of a document, the court, if necessary, may order the party to produce the document and examine it in private.[22]

Judgments or rulings made by a foreign court that requests a person in Taiwan to produce documents will automatically be recognised in Taiwan unless one of the circumstances outlined in Article 402 Paragraph 1 of the Code of Civil Procedure exists.-[23] However, foreign courts must obtain a judgment of approval in accordance with Article 4-1 Paragraph 1 of the Compulsory Enforcement Act before requesting compulsory enforcement from Taiwan's courts.

Communication surveillance for national security and major crimes

The CSSA was enacted in 1999 and revised on 12 July 2024 to protect the freedom of private communication and privacy, ensure national security and maintain social order.[24] It stipulates that the government may only engage in communication surveillance where it is necessary for ensuring national security and maintaining social order.[25]

Police and prosecutors must obtain an interception warrant from courts to monitor telecommunications, emails, letters, speeches and conversations in a criminal investigation. An interception warrant may only be issued for the investigation of major crimes with a minimum sentence of three years or above or other specified crimes that threaten national security or the socioeconomic order, where it is reasonable to believe the contents of the monitored telecommunication are relevant to the case, and such contents are difficult or impossible to obtain elsewhere.[26]

With respect to communication surveillance to collect intelligence of foreign forces or hostile foreign forces, an interception warrant is issued by the head of the National Security Bureau, and the information obtained from such surveillance may only be used for national security unless it fulfils the requirements for criminal communication surveillance.[27]

There are limitations to how the communication surveillance is conducted and how the information is used. For example, permissible communication surveillance does not include setting up tapping devices, video recording equipment, or other monitoring equipment in private dwellings.[28] Further, recorded content clearly unrelated to the purpose of the surveillance may not be transcribed[29]. Finally, information obtained according to the CSSA may not be provided to other institutions, groups, or persons unless otherwise stipulated by law.[30]

The CSSA also states that the police or prosecutors must request an access warrant from the court to obtain communication records and network traffic records from telecommunication services, and that there are facts supporting the belief that such user information and communication records are necessary and relevant to the case.[31]

Public and private enforcement

Enforcement agencies

Taishin International Bank was fined NT$6 million by the FSC for deficiencies in internal controls and inadequate oversight of outsourced service providers. The Financial Supervisory Commission (FSC) found that unsynchronised system adjustments and

insufficient testing procedures led to errors in billing address data and mismatches between customer names and transaction details. These failures resulted in potential personal data breaches affecting 1,447 customers. The bank was found to have violated the Banking Act and relevant internal control regulations.[32]

Private litigation

Compared to other jurisdictions, there are relatively few cases in Taiwan where private plaintiffs have claimed damages because of personal data violations (including personal and class action suits). There have been no leading cases in the past two years that may set important precedents.

Considerations for foreign organisations

Foreign entities must comply with the PDPA when collecting, processing and using personal data within Taiwan's borders.[33] If the foreign entity does not have an establishment in Taiwan (such as a branch), the PDPA will apply to the natural person, such as an employee, who actually engaged in the collection, processing or use of the personal data in Taiwan.[34]

As mentioned under the heading 'International data transfer and data localisation' and subject to the restrictions noted therein, cross-border transfer of information is generally permissible as long as the collection, processing and use of personal data is legal. Therefore, there is no requirement that personal data be exclusively stored in Taiwan, and organisations may, subject to limited exceptions, be transferred outside of Taiwan.

Cybersecurity and data breaches

The CSMA was enacted on 6 June 2018 to proactively promote national information security policies, create a safe environment in the country and defend the public interest. The CSMA, along with its sub-regulations, applies to government agencies[35] and non-government agencies,[36] as defined therein.

Appointing a chief information security officer

Government agencies are to appoint a cybersecurity officer responsible for carrying out and overseeing the cybersecurity business of the agency.[37] Specific industries are also required to have an information security supervisor; for example, enterprises in the banking industry must establish an information security specialised unit and appoint a supervisor who does not have a conflict of interest with their other duties.[38]

Information communication security

Government and non-government agencies are required to meet the cybersecurity requirement level applicable to them under the CSMA and to take into account the category,

quantity, and attributes of the information reserved or processed, along with the scale and attributes of the information and communication system, to stipulate, amend and implement the cybersecurity maintenance plan.[39] Security maintenance plans should include the following:

1. the goals and regulations of the information security policy;
2. the cyber security policy and objectives;
3. the organisation, persons in charge, and budgeting plans;
4. the deployment of cyber security officer of the government agency;
5. an inventory of the information and information communication system;
6. a risk assessment of information communication security;
7. a protocol for information security protection and control;
8. mechanisms for notification, crisis management, and rehearsal in the case of a security breach;
9. an assessment of and response to information communication security;
10. management of outsourced projects;
11. training;
12. testing for members of governmental agencies on information communication security; and
13. a management and continuous improvement plan.[40]

Implementation of personal data security

Central competent authorities may mandate non-governmental agencies to establish plans for maintaining personal data security and disposal of such information after the termination of the project.[41] As of 14 July 2025, 59 industries have been designated to set up the relevant plans and processing methods.[42] These companies in these industries are required to keep and implement the following security protocols: establish guidelines for using various types of equipment or media storage and establish appropriate measures to prevent information leaks when they are disposed of or used for other purposes; encrypt personal data that needs to be encrypted when collecting, processing or using such information; and take appropriate safety precautions when a personal data file needs to be duplicated.[43]

Mechanisms for notification and crisis management in the case of a security breach

In the case of a security breach, governmental and non-governmental agencies must notify their superiors and supervisory institutions, as well as the relevant competent authorities. In addition, governmental agencies must provide an investigative analysis report and plans for improvement to superiors and supervisory institutions. Non-governmental agencies must formulate appropriate methods of informing subjects when their personal data is stolen, tampered with, damaged, destroyed, or leaked. The notification to the data subjects

shall include the facts of the security breach, the current crisis management, and the number for an advisory service line.[44]

Digital governance and convergence with competition policy

In response to the rise of the digital economy, the Taiwan Fair Trade Commission (TFTC) published the White Paper on Competition Policy in the Digital Economy in December 2022 and further revised it in December 2023. In the White Paper, the TFTC pointed out several competition issues in the digital economy, including the challenges to traditional market definition and assessment of market power, self-preferencing and search bias, tie-in sale, predatory pricing/inducement with low price, price discrimination, Most Favored Nation (MFN) Clauses, resale price maintenance, online sales channels restriction, data privacy and market competition, advertisement revenue sharing with news media, killer acquisitions, algorithm and concerted, and false online advertising.[45] Further, for each competition issue, the White Paper compiled foreign and domestic experience and the concerns and challenges faced, as well as the TFTC's possible enforcement positions and guiding principles.

For the issue of data privacy and market competition, the White Paper indicated that although the TFTC has not addressed any cases where the Fair Trade Act has been used to tackle privacy infringements by platform operators who collect or use personal data, the TFTC will continue to follow the discussions and development of this issue both domestically and internationally.

In addition to the White Paper, the TFTC also amended the Principles of the Fair Trade Commission Regarding the Definition of the Relevant Markets, adding definitions and revising consideration factors for the definition of the product market and the geographic market related to the digital economy.[46]

Outlook and conclusions

The *111-Xian-Pan-Zi No.13* Constitutional Decision of 12 August 2022 held that the secondary use of personal data in the health insurance database is partially unconstitutional. The Constitutional Court found that there was a lack of an independent supervisory mechanism for personal data protection in Taiwan and ordered the competent authority to amend the regulations to include such a mechanism within three years of the announcement of the decision. In response to the Constitutional Decision, the PDPA was amended on 31 May 2023 to establish a single competent authority for the supervision of the PDPA, namely the PDPC. The preparatory office of the PDPC was established on 5 December 2023 to assume the functions previously performed by the NDC and to oversee the planning, coordination and promotion of the PDPC's establishment as well as the revision and interpretation of the PDPA.

Endnotes

1 The PDPA recognises the terms government agency and non-government agency that collect, process or use personal data instead of data controller. ^ Back to section

2 PDPA, Article 5. ^ Back to section

3 PDPA, Article 15. ^ Back to section

4 PDPA, Article 19. ^ Back to section

5 PDPA, Article 18 and Article 27, Paragraph 1. ^ Back to section

6 PDPA, Article 27 Paragraph 2. ^ Back to section

7 PDPA, Article 3. ^ Back to section

8 PDPA, Article 11. ^ Back to section

9 ESA, Article 5. ^ Back to section

10 The competent authorities that joined the CPEA are the Ministry of the Interior, Ministry of Foreign Affairs, Ministry of Education, Ministry of Justice, Ministry of Economic Affairs, Ministry of Transportation and Communications, Ministry of Labour, Council of Agriculture, Ministry of Health and Welfare, Ministry of Culture, Ministry of Science and Technology, Financial Supervisory Commission (FSC), Public Construction Commission, Fair Trade Commission and NCC. ^ Back to section

11 Under the Regulations Governing Security of Personal Data Kept by Non-Governmental Agencies designated by the FSC, these non-government agencies include financial holding companies, the banking industry, the securities and futures industry, the insurance industry, the electronically stored value card industry, electronic payment institutions and other financial service industries approved by the FSC. ^ Back to section

12 Under the Regulations Governing Security of Personal Data Kept by Non-Governmental Agencies designated by the NCC (applies to non-government agencies, including telecommunications businesses, public telecommunications network operators that provide Internet access services and do not use telecommunications resources and have more than 3,000 users, cable broadcasting and television system operators, television businesses, live satellite broadcasting businesses with over 3,000 subscribers, domestic news channels, shopping channel satellites, or other channel programme supplying businesses, telecommunications dispute resolution institutions, and other communications businesses announced by the NCC). ^ Back to section

13 The Regulations Governing Security of Personal Data Kept by Non-Governmental Agencies designated by NCC, Article 3. ^ Back to section

14 id., Article 5. Back to section

15 id., Article 4. Back to section

16 id., Article 6. Back to section

17 Regulations Governing Security of Personal Data Kept by the Copyright Collective Management Organization designated by the Ministry of Economic Affairs. Back to section

18 Enforcement Rules of ESA, Article 1-1, Paragraph 2. Back to section

19 ESA, Article 5, Paragraph 2, Subparagraph 2. Back to section

20 Code of Civil Procedure, Article 341. Back to section

21 Code of Civil Procedure, Article 342, 343, 346 and 347. Back to section

22 Code of Civil Procedure, Article 344, Paragraph 2. Back to section

23 Order of Judicial Yuan, Secretary-General, No 1070030760. Back to section

24 CSSA, Article 1. Back to section

25 CSSA, Article 2, Paragraph 1. Back to section

26 CSSA, Article 5. Back to section

27 CSSA, Article 7 and 10. Back to section

28 CSSA, Article 13, Paragraph 1. Back to section

29 CSSA, Article 13, Paragraph 4. Back to section

30 CSSA, Article 18, Paragraph 1. Back to section

31 CSSA, Article 11-1. Back to section

32 See the administrative sanctions imposed by the FSC, at https://www.fsc.gov.tw/ch/home.jsp?id=131&parentpath=0,2&mcustomize=multimessages_view.jsp&dataserno=202505090002&dtable=Penalty. Back to section

33 Reference in the letter of the Ministry of Justice No. 10100088140 dated 6 June 2013. Back to section

34 PDPA, Article 2, Paragraph 8. Back to section

35 Government agencies are defined under CSMA, Article 3, Paragraph 5, as central and local institutions or legal persons that exercise public power in accordance with the law but specifically exclude military and intelligence agencies. ^ Back to section

36 Non-government agencies are defined under CSMA, Article 3, Paragraph 6, and include critical infrastructure providers, government-owned enterprises and government-endowed foundations. ^ Back to section

37 CSMA, Article 11. ^ Back to section

38 Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries, Article 38-1. ^ Back to section

39 CSMA, Article 10, and Article 16, Paragraph 2, and Article 17, Paragraph 1. ^ Back to section

40 Enforcement Rules of Cyber Security Management Act, Article 6, Paragraph 1. ^ Back to section

41 PDPA, Article 27, Paragraph 2. ^ Back to section

42 See the Preparatory Office of the Personal Data Protection Commission, https://www.pdpc.gov.tw/CP/130/. ^ Back to section

43 The Regulations Governing Security of Personal Data Kept by Non-Governmental Agencies designated by the FSC, Article 9. ^ Back to section

44 The Regulations Governing Security of Personal Data Kept by Non-Governmental Agencies designated by the FSC, Article 6, Paragraph1. ^ Back to section

45 https://www.ftc.gov.tw/upload/bcfbee8b-2ed0-494d-a993-c8a5506d5752.pdf. ^ Back to section

46 https://www.ftc.gov.tw/internet/main/doc/docDetail.aspx?uid=1345&docid=13926. ^ Back to section

理慈 Lee, Tsai & Partners

Jaclyn Tsai Jaclyntsai@leetsai.com
Jaime Cheng jaimecheng@leetsai.com
Hannah Kuo hannahkuo@leetsai.com

Lee Tsai & Partners