PANORAMIC

DATA PROTECTION & PRIVACY

Taiwan

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: August 4, 2025

Contents

Data Protection & Privacy

SHARING AND CROSS-BORDER TRANSFERS OF PI

RIGHTS OF INDIVIDUALS

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

SPECIFIC DATA PROCESSING

UPDATE AND TRENDS

Contributors

Taiwan

Formosa Transnational Attorneys at Law

萬國法律事務所 Formosa Transnational Attorneys at Law

Yulan Kuo	yulan.kuo@taiwanlaw.com
Jane Wang	jane.wang@taiwanlaw.com
Brian Hsieh	brian.hsieh@taiwanlaw.com
Emily Hsu	emily.hsu@taiwanlaw.com

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

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

The PDPA does not explicitly cite any foreign legislation. However, according to the historical record, the drafters of the PDPA did consider the provisions of EU Directive 95/46/EC (the Data Protection Directive), the Organization for Economic Cooperation and Development Guidelines and the Asia-Pacific Economic Cooperation's privacy framework when drafting the PDPA.

Law stated - 27 6 2025

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

Prior to 2023, the PDPA did not give any single governmental agency overriding authority to oversee enforcement of the Act. As such, there was no particular governmental agency in Taiwan actively policing personal data protection practices.

On 31 May 2023, Taiwan's legislature amended the PDPA. Under the 2023 Amendments, the Personal Data Protection Commission (PDPC), a newly established regulatory agency, will be responsible for overseeing the PDPA's enforcement in Taiwan. The PDPC will be an independent data protection authority that carries out regulatory functions in relation to personal data protection in Taiwan.

On 5 December 2023, Taiwan's Executive Yuan inaugurated a PDPC preparatory office. This newly established office will play a crucial role in drafting and amending regulations related to PI and the PDPC's organisation act.

Law stated - 27 6 2025

Cooperation with other data protection authorities

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

Prior to 2023, the PDPA did not give any particular governmental agency overriding authority to enforce data protection law, but the PDPA does require the Ministry of Justice to set forth guiding principles. However, after the establishment of the PDPC, of which operation date will otherwise be designated by the Taiwan authority, the PDPC shall have the sole authority to set forth guiding principles.

Law stated - 27 6 2025

Breaches of data protection law

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

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

The competent authority could impose upon the breaching entity a cease-and-desist order that compels the breaching entity to immediately cease collecting, processing and using the relevant PI. The agency could also order the breaching entity to delete the PI possessed by the breaching entity, or to confiscate or destroy the PI that the breaching entity unlawfully collected. The agency may also publish the facts of such a data breach and the name of the breaching entity and its representative.

Administrative penalties may be a fine imposed on the breaching entity and its representative of between NT$20,000 and NT$15 million.

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

Law stated - 27 6 2025

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Where an order is imposed on a PI owner regarding PI matters by the competent authority and the PI owner disagrees with this order, which may be against the PI owner's interests, it may file an administrative appeal to the administrative appeal committee of the competent authority, requesting that the committee reconsider the order. The PI owner can bring the same matter to the courts if it subsequently fails to receive a favourable decision from the committee.

Law stated - 27 6 2025

SCOPE

Exempt sectors and institutions

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

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

Law stated - 27 6 2025

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

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

Law stated - 27 6 2025

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

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

Law stated - 27 6 2025

PI formats

What categories and types of PI are covered by the law?

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

Law stated - 27 6 2025

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The PDPA explicitly provides that a Taiwan entity or individual will be subject to the obligations set forth by the PDPA for their use, collection or processing of PI of other Taiwan citizens outside the territory of Taiwan. According to the explanatory decree by the Ministry of Justice of Taiwan, if the use, collection or processing of PI occurs outside the territory of Taiwan, the following requirements must be met before the PDPA becomes applicable: the entity engaging in the collection, processing or use of PI is a government agency or non-government entity 'established in Taiwan'; and the PI subject is a Taiwan citizen.

Law stated - 27 6 2025

Covered uses of PI

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

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

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

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

Law stated - 27 6 2025

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

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

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

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

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

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

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

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

- the exemption from the obligation to disclose is permitted by law;
- the collection of PI is necessary for a government agency to perform its official duties or for a non-government entity to fulfil a legal obligation;

- the disclosure will impede a government agency in performing its official duties;
- the disclosure will impair the public interest;
- the PI subject should have already known the content of the notification; and
- the collection of personal information is for non-profit purposes, and it will not harm the interests of the data subject.

Law stated - 27 6 2025

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

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

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

Law stated - 27 6 2025

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Yes, under the Personal Data Protection Act (PDPA), if the personal information (PI) is collected without the consent of the data subject, the PI owner is required to notify the data subject of its possession of their PI before the owner processes or uses the PI. The notice must include the following information:

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

Law stated - 27 6 2025

Exemptions from transparency obligations

When is notice not required?

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

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

Law stated - 27 6 2025

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

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

Law stated - 27 6 2025

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

The PDPA does not restrict the volume of PI that may be collected, and the PDPA imposes more stringent rules to restrict the collection, processing and use of the sensitive PI.

Law stated - 27 6 2025

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The PDPA does not restrict the amount of PI that may be held or the specific length of time it may be held. Nevertheless, the PDPA requires the PI owner to cease processing or using the PI once the specific purpose of the collection, processing or use of the PI no longer exists or the term of such purpose has expired. However, if processing or using the PI is necessary to perform official duties or to fulfil legal obligations, or is consented to by the data subject, the PI owner may continue to process or use the PI.

Law stated - 27 6 2025

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

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

The PDPA stipulates that when a data subject's PI is collected, the data subject must be expressly informed of the purpose of the collection, and the processing or use of the PI must

be performed in connection with the purpose. In addition, there are some exceptions to the purpose limitation principle. The PDPA allows PI to be used for new purposes if any one of the following situations exists:

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

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

Law stated - 27 6 2025

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

No. Currently, the PDPA does not provide any provisions regarding automated decision-making.

Law stated - 27 6 2025

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

A government agency or non-government entity keeping possession of any personal information (PI) privacy by design must adopt appropriate cybersecurity measures to prevent the PI from being stolen, altered, damaged, destroyed or disclosed. If the PI owner is a government agency, it is required to assign specific persons to be in charge of the security of PI. Also, the Personal Data Protection Act (PDPA) Enforcement Rules provide guidelines for such security measures. For example, the PI owner may assign and allocate personnel to manage PI, establish a mechanism to evaluate risk, prevent leaks, deal with any accidental incidents, establish internal rules, hold educational training and maintain the security system for regular periods. Moreover, the central government may require specific non-government

entities to stipulate internal principles to protect the safety of PI, including how PI will be disposed of after the termination of the relevant business.

Law stated - 27 6 2025

Notification of data breach

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

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

Law stated - 27 6 2025

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

A government agency or non-government entity must adopt appropriate security and maintenance measures, including, without limitation, establishing internal rules and preserving use records and relevant evidence. In particular, some specific non-government entities, including in the banking and medical sectors, must conduct much stricter obligations requested by relevant personal information (PI) regulations to strengthen internal data control.

The Personal Data Protection Act (PDPA) stipulates that the relevant government authorities may inspect compliance with the security control measures, the guidelines on disposing of personal data upon business termination and the restrictions on cross-border transfers, and may conduct any other routine inspections when they deem it necessary to suspect any possible violation. They may also order relevant personnel of the non-government agencies to provide necessary explanations or supporting documents.

Law stated - 27 6 2025

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

Under the PDPA, a government agency keeping possession of PI is required to appoint a data protection officer (DPO), but this does not apply to a non-government entity. The responsibility of the DPO is to prevent PI from being stolen, altered, damaged, destroyed or disclosed. However, the guidelines for security measures afforded by the PDPA Enforcement Rules suggest that a non-government entity appoint a DPO to manage the PI that it possesses. Also, some relevant PI regulations specifically applied to particular industries require PI owners to appoint a DPO. For example, the regulations respectively applicable to banks, insurance providers, short-term educational centres and medical sectors require entities in these industries to appoint a DPO.

Law stated - 27 6 2025

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

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

Law stated - 27 6 2025

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The PDPA does not address risk assessments for privacy impacts. However, the PDPA Enforcement Rules suggest that PI owners or processors, whether government or non-government entities, establish a mechanism to assess the risk of collecting, processing and using PI. Some relevant PI regulations specifically applied to particular industries further require PI owners or processors to periodically conduct risk assessments on their collection, processing or use of PI. For example, online shops and platforms, banks and insurance providers, real estate agencies, and short-term educational centres are obliged to conduct such PI risk assessments. Notwithstanding the foregoing, these regulations and rules do not provide clear definitions or substantial requirements for conducting risk assessments in practice.

Law stated - 27 6 2025

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

The PDPA does not provide for obligations in relation to how PI processing systems must be designed, such as privacy- by-design.

Nonetheless, some industry-specific regulations apply to businesses, such as banks and insurance providers, and require such regulated enterprises to implement appropriate technical measures and make reasonable distribution of operational resources to planning, establishing, reviewing and revising these measures based on the scale and characteristics of their business.

For example, if PI owners or processors provide e-commerce platform services, they should adopt information security measures at a specific level, including a user identity confirmation and protection mechanism, a security encryption mechanism for Internet data transmission, and measures for restriction and monitoring of PI files and databases.

Law stated - 27 6 2025

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

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

Law stated - 27 6 2025

Other transparency duties

Are there any other public transparency duties?

Under the Personal Data Protection Act, a government agency is required to publish the following information on the internet or by other proper means for review:

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

Non-government entities keeping PI are not obliged to make such publication.

Law stated - 27 6 2025

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

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

Law stated - 27 6 2025

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Disclosing PI to other recipients, whether based on selling PI or sharing for targeted advertising purposes, must all be done under the regulations for the use of PI under the PDPA. That is, for a non-government entity, if disclosing PI to other recipients is within the scope of a specific purpose for collecting and processing the PI, the PI owner may freely make such disclosure. Otherwise, the disclosure can be made only if it satisfies the requirements under which the use of PI for new purposes is allowed. However, the recipient must notify the data subject of its possession of the PI before processing or using the PI, except when the data subject has been properly notified of the recipient's use or processing of the PI when the PI is collected.

Law stated - 27 6 2025

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

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

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

For example, the Taiwan National Communications Commission has issued an order to forbid communications enterprises from transferring their users' personal data to mainland China. In 2022, the Ministry of Health and Welfare also issued an order to forbid the social worker's office to transfer PI to mainland China.

Law stated - 27 6 2025

Further transfer

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

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

Law stated - 27 6 2025

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

While the PDPA itself does not specifically require data localisation, regulations relating to financial institutions do. For example, under the 'Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation', the PI outsourced to a cloud service provider must be processed and stored within the territories of Taiwan in principle. If the PI is processed and stored outside Taiwan, the following rules shall be applied:

- the financial institution shall retain rights to designate the location for the processing and storage of the data;
- the data protection regulations in such jurisdiction must not be lower than the requirements of Taiwan; and
- except with the approval of the competent authority, copies of PI must be retained in Taiwan.

Law stated - 27 6 2025

RIGHTS OF INDIVIDUALS

Access

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

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

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

Law stated - 27 6 2025

Other rights

Do individuals have other substantive rights?

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

Law stated - 27 6 2025

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes. Data subjects are entitled to monetary damages if their PI is breached, as follows:

- Compensation is not limited to loss of costs, as non-pecuniary damages such as emotional distress and loss of reputation are available. If the reputation of the PI subject is harmed owing to the PI owner's breach of the PDPA, the PI subject may request the court to order the PI owner to restore their reputation.
- If the data subject has difficulty establishing the actual damages caused by the breach, they may request the court to grant compensation of an amount of no less than NT$500 but no more than NT$20,000 for each breach.
- If the breach causes damages to multiple data subjects by the same cause and fact, those victims are entitled to monetary compensation of no more than NT$200 million. However, if the value of the interests the breaching party may gain from the alleged violation is higher than NT$200 million, the victims are entitled to monetary compensation of no more than the established value of said interests.
- If the damages to multiple data subjects by the same cause and fact exceed NT$200 million, the limitation on compensation granted of the amount of no less than NT$500, as provided under the condition specified in the second bullet point above, shall not apply.

- Statute of limitation: the right to claim compensation will be blocked after two years from the date on which the data subject became aware of the damages and of the person who is liable for the damages, or five years from the date of the occurrence of the damage.

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

Law stated - 27 6 2025

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

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

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

If the PI owner is a government agency, data subjects must file an administrative appeal against this government agency and, if not successful, then file an administrative lawsuit.

Law stated - 27 6 2025

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions
Does the law include any derogations, exclusions or limitations other than those already described?

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

Law stated - 27 6 2025

SPECIFIC DATA PROCESSING

Cookies and similar technology
Are there any rules on the use of 'cookies' or equivalent technology?

The Personal Data Protection Act (PDPA) does not contain specific provisions to regulate the use of cookies. However, if the information collected through cookies matches the

definition of personal information (PI), the PDPA shall apply. Taking distributing targeted advertisements, for example:

- when the server collects PI from an individual, it must comply with the rules regulating PI collection under the PDPA;
- when the server analyses the PI collected, it must comply with the rules regulating PI processing and use under the PDPA; and
- when the server uses its analysing report to distribute targeted advertisements, it must comply with the rules regulating PI use under the PDPA.

In this regard, more and more websites utilise a pop-up window seeking users' consent to the collection, processing and use of their PI when the user visits the website for the first time.

Law stated - 27 6 2025

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Under the PDPA, when a non-government entity uses the PI collected to do marketing, regardless of whether it is via email, fax, telephone or other electronic forms, it must stop if the data subject so requires. Also, when PI is first used by a non-government entity for marketing, the data subject must be advised of the measures for declining such marketing use. The expense for carrying out these measures must be borne by that entity.

Law stated - 27 6 2025

Targeted advertising

Are there any rules on targeted online advertising?

The PDPA and its related regulations do not provide specific provisions for targeted advertising. However, the advertising provider must comply with the general rules under the PDPA when collecting, processing and using the PI.

Law stated - 27 6 2025

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

Yes. Sensitive PI can only be collected, processed and used in the following situations:

- the collection, processing and use of PI is permitted by law;
- the collection, processing and use of PI is necessary for a government agency to perform its official duties or for a non-government entity to fulfil a legal obligation,

and proper safety measures are taken during and after the collection, processing and use of PI;

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

Law stated - 27 6 2025

Profiling

Are there any rules regarding individual profiling?

No. Currently, the PDPA does not specify any rules regarding individual profiling.

Law stated - 27 6 2025

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

The PDPA does not contain specific provisions that regulate the use of cloud computing services. The use of cloud computing services must comply with all rules regulating the collection, processing and use of PI under the PDPA. Cloud services might trigger the following two issues under the PDPA:

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

territories of Taiwan in principle. If the PI is processed and stored outside Taiwan, the following rules shall be applied:

- the financial institution shall retain rights to designate the location for the processing and storage of the data;
- the data protection regulations in such jurisdiction must not be lower than the requirements of Taiwan; and
- except with the approval of the competent authority, copies of PI must be retained in Taiwan.

Law stated - 27 6 2025

UPDATE AND TRENDS

Key developments of the past year

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

The Personal Data Protection Act (PDPA) was amended in 2023 to establish the Personal Data Protection Commission (PDPC). Since 2023, the amendment of the PDPA has drawn sustained public attention. The reform not only responds to global demands for stronger data protection but also addresses the Constitutional Court's call for an independent supervisory framework.

In March 2025, the Executive Yuan approved a draft amendment to the PDPA, which is currently under review by the Legislative Yuan. This 2025 draft significantly strengthens Taiwan's regulatory framework for personal data protection, particularly across both public and private sectors. Notably, it introduces – for the first time in Taiwan – the role of a data protection officer within public agencies to oversee and promote compliance with data protection regulations.

With respect to the private sector, this 2025 draft amendment sets out clear requirements for personal data breach notification. Moreover, recognising the longstanding fragmentation of regulatory oversight among various competent authorities, the draft amendment designates the PDPC as the unified supervisory authority for private entities. To facilitate a stable transition, the draft amendment introduces a transitional period, currently set at six years. Following the establishment of the PDPC, priority will be given to the supervision of public sector entities and private entities that currently do not fall under a specific competent authority. As for private entities already under the jurisdiction of designated central competent authorities, the existing supervisory structure will remain unchanged during the transition period.

The formation of the PDPC and the enactment of the 2025 amendment are expected to be completed by August 2025.

Law stated - 27 6 2025