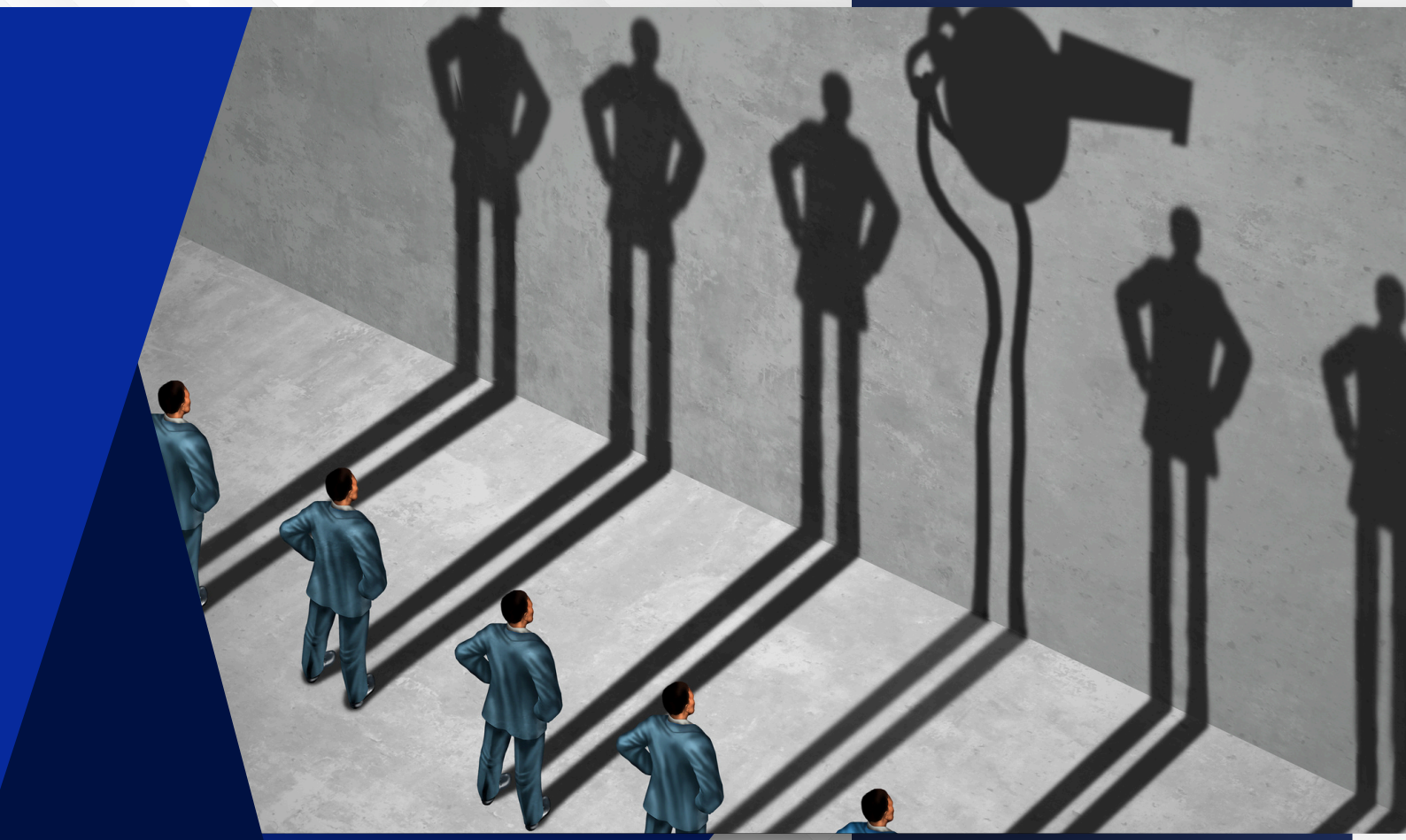
iLAW
ASIA



GUIDELINES

PDPA WHISTLEBLOWER 2025

DATE:
15 July 2025

CAMBODIA
ILAW Cambodia Law Office

CHINA
Kingbridge Sun Kuong Law Firm

HONG KONG
Sun Lawyers LLP

INDONESIA
ADCO Law

JAPAN
Japan Desk at ILAWASIA

LAOS
ILAW Laos

TAIWAN
TaipeiLaw Attorneys-at-Law

THAILAND
ILAWASIA

VIETNAM
CDLAF Law Firm

About the Guidelines

ILAWASIA, in collaboration with a network of esteemed partner law firms, is proud to present the **PDPA Whistleblower Guidelines**, designed to offer in-depth insights into data protection and whistleblower regulations across selected jurisdictions. These guidelines have been meticulously curated to support business stakeholders in understanding the legal landscape of countries with emerging and strategic market potential.

Through this initiative, we aim to provide a comprehensive overview of key regulatory frameworks, enforcement mechanisms, and compliance obligations relevant to whistleblower protection under personal data protection laws. The guidelines cover a wide range of topics, including:

- Legal definitions and scope of whistleblower protection.
- Reporting channels and confidentiality safeguards.
- Employer obligations and employee rights.
- Cross-border data transfer considerations.
- Enforcement authorities and penalties for non-compliance.

Our goal is to empower clients with the knowledge and clarity needed to navigate the complexities of cross-border data protection and whistleblower regulations. By equipping businesses with practical legal insights, we enable informed decision-making and strategic planning in their international operations.

Table of Contents

Foreword from Our Partner

In today's interconnected digital landscape, the protection of personal data is not just a legal obligation—it is a shared responsibility that transcends borders. As organizations navigate the complexities of data privacy laws across Asia, regional collaboration becomes essential to ensure compliance, transparency, and trust.

We are proud to present this PDPA Whistleblower initiative as a result of close cooperation with our trusted legal partners across Asia. Through formal Memorandums of Understanding (MOUs), we have built a strong network of law firms that bring deep local expertise and a shared commitment to upholding the highest standards of data protection.

Participating firms in this collaboration include:

- Cambodia – ILAW Cambodia Law Office
- China – Kingbridge Sun Kuong Law Firm
- Hong Kong – Sun Lawyers
- Indonesia – ADCO Law Firm
- Japan – Japan Desk at ILAWASIA
- Laos – ILAW Laos
- Taiwan – TaipeiLaw Attorneys-at-Law
- Thailand – ILAWASIA
- Vietnam – CDLAF Law Firm

Each of these firms plays a vital role in shaping the regional dialogue on data privacy. Their insights have been instrumental in tailoring this initiative to reflect the legal, cultural, and operational realities of their respective jurisdictions. From advising on local whistleblower protections to interpreting the nuances of PDPA implementation, their contributions ensure that this publication is not only comprehensive but also practical and actionable.

This collaboration reflects our shared vision: to empower individuals and organizations with the knowledge and tools needed to report data breaches and unethical practices safely and effectively. By working together, we aim to foster a culture of accountability and integrity across Asia.

We extend our sincere gratitude to our partners for their unwavering support and dedication. Together, we are building a stronger, more transparent future for data governance in the region.

Editorial Team

Tanadee Pantumkomon
Project Supervisor

Nisapan Chinnwiicha
Project Coordinator

Ploypisut Punbura
Coordinator

Tanadee Pantumkomon
Partner, ILAWASIA

PDPA Whistleblower in Cambodia

As Cambodia advances its Personal Data Protection Law, the inclusion of whistleblower protections is vital to ensure transparency and accountability.

In collaboration with ILAW Cambodia Law Office, we advocate for legal safeguards that empower individuals to report data misuse without fear of retaliation—building public trust in the digital age.

PDPA Whistleblower

CAMBODIA

What is the primary law governing personal data protection in your jurisdiction? Provide a summary of its Application.

The primary and highest-ranking legal instrument governing the Personal Data Protection Act (PDPA) in Cambodia is the 1993 Constitutional Law of Cambodia. By the paragraph 1 of Article 32 states that "**Every Khmer citizen shall have the right to life, personal freedom, and security**". As of March 13, 2025, the Personal Data Protection Act (PDPA) in Cambodia remains in draft form and has not yet been enacted. The draft is currently being developed by the Ministry of Post and Telecommunications (MPTC). In the absence of an official PDPA, personal data in Cambodia is currently protected under the Constitution and existing laws, such as the Law on Telecommunications (2015), the Criminal Code (2009), the Civil Code (2007), the Law on Electronic Commerce (2019), and other related regulations.

Under these legal provisions, the definition of personal data varies depending on the specific law governing the information, and the associated penalties may differ across the relevant laws and regulations. The following sections outline the details of personal data protection as governed by various laws and regulations, including relevant definitions, penalties and what must a business do after a personal data breach.

What measures should businesses take in the event of a personal data breach?

In the event of a personal data breach, businesses are required to take appropriate measures to minimize the impact and comply with legal obligations. This includes conducting an internal investigation to determine the cause of the breach and whether it resulted from employee actions. Based on the findings, the business should seek to resolve the matter with the involved parties through Alternative Dispute Resolution (ADR) methods. However, in cases involving large-scale data breaches or doxxing that cannot be resolved through ADR, the business may file a criminal complaint with the Department of Anti-Cybercrime under the Ministry of Interior for further investigation by Judicial Police Officers (Officier de Police Judiciaire – OPJ) or submit the case directly to the court to pursue criminal charges and claim damages against the offender.

What are the penalties for non-compliance with personal data protection laws?

A. PDPA under the Criminal Code of Cambodia

According to Article 314 of the Criminal Code of Cambodia (2009), a personal data breach occurs when a person, by virtue of their position, profession, duties, or mission, is entrusted with confidential information and discloses it to someone who is not authorized to receive it. Although the Code does not explicitly mention personal data breaches, such actions are considered breaches of professional secrecy. In cases involving certain positions or professions, these actions may also constitute personal data breaches. As a criminal offense, they are punishable by imprisonment ranging from 1 month to 1 year, and a fine between 100,000 and 2,000,000 riels (approximately USD 25 to USD 500).

Authors

Tanadee Pantumkomon
Partner
Tanadee.P@ilawasia.com

Hort Lypheng
Legal Clerk
ilawcambodia@ilawasia.com

Contact

ILAW CAMBODIA LAW OFFICE
#89A, Level 1, St.294, Phum3,
Sangkat Boeung Keng Kan I,
Khan Boeung Keng Kang,
Phnom Penh, Cambodia.

Tel: +855 12 327 669
Email: ilawcambodia@ilawasia.com

Additionally, under Article 318 of the Criminal Code also addresses breaches of privacy in telephone conversations, which may fall under personal data breaches. This includes actions such as maliciously listening to or interfering with phone calls. As a criminal offense, such acts are punishable by imprisonment from 1 month to 1 year and a fine ranging from 100,000 to 2,000,000 riels (approximately USD 25 to USD 500).

B. PDPA under the Civil Code of Cambodia

The Civil Code of Cambodia (2007) protects personal data as part of an individual's rights. These rights include life, personal safety, health, freedom, identity, dignity, privacy, and other personal interests[1]. If someone's individual rights are unlawfully violated, they have the legal right to stop the violation[2], request the removal of its effects[3], and claim compensation for any harm caused[4].

C. PDPA under the Law on Telecommunications

Telecommunication laws also focus on protecting personal data. Anyone who secretly listens to or records a conversation using a personal telecommunication system without the consent of the other person can face imprisonment for 1 month to 1 year and a fine of 100,000 to 2,000,000 Riels (approximately USD 25 to USD 500). The same penalties apply if the content of the conversation is made public without legal consent from the parties involved, a legitimate authority, or applicable legal regulations. However, this does not apply if the recording or listening is done with the consent of the people involved or with approval from a legitimate authority[5].

On the other hand, this law also addresses doxxing. If someone uses a third party's identity on a telecommunication system in a way that leads to or could lead to criminal charges against them, they can face imprisonment from 1 to 3 years and a fine of 2,000,000 to 6,000,000 Riels (approximately USD 500 to USD 1,500).

D. PDPA under the Law on Electronic Commerce

In the context of e-commerce, the Law on Electronic Commerce (2019) also addresses personal data protection. It requires that any person holding personal information in electronic form must take all reasonable measures to safeguard it from loss, unauthorized access, use, modification, leakage, or disclosure—except with the consent of the data owner or as permitted by law. Furthermore, no person shall, in bad faith or without authorization, interfere with an electronic system or access, retrieve, copy, extract, leak, delete, or modify data held by another person[6].

Non-compliance with personal data protection obligations under this law may result in criminal penalties, including imprisonment from 1 to 2 years and a fine ranging from 2,000,000 to 4,000,000 riels[7] (approximately USD 500 to USD 1,000).

CONCLUSION

Although Cambodia has not yet enacted a dedicated Personal Data Protection Act (PDPA), existing legal frameworks provide various protections for personal data through the Constitution, the Criminal Code, the Civil Code, the Law on Telecommunications, and the Law on Electronic Commerce. These laws define different aspects of personal data, outline obligations for data handlers, and impose penalties for misuse or breaches. In the absence of a unified PDPA, businesses must remain vigilant in handling personal data, especially in the event of a breach. They are expected to conduct internal investigations, resolve disputes through appropriate channels such as ADR, and, when necessary, escalate serious cases to the authorities for legal action. Until a formal PDPA is adopted, compliance with existing laws remains essential for upholding the rights to privacy, data security, and personal dignity in Cambodia.

At ILAWASIA, we offer expert legal counsel on the Personal Data Protection Act compliance, including litigation process for any breach under the Personal Data Protection Act, assisting businesses in navigating their regulatory obligations with confidence. If you need guidance on incident notification, filing complaints, or any other the Personal Data Protection Act-related matters, please contact us for further consultation.

[1]Article 10 of Law on Civil Code of Cambodia 2007
[2]Article 11 of Law on Civil Code of Cambodia 2007
[3]Article 12 of Law on Civil Code of Cambodia 2007
[4]Article 13 of Law on Civil Code of Cambodia 2007
[5]Article 97 of Law on Telecommunication 2015
[6]Article 32 of Law on Electronic Commerce 2019
[7]Article 60 of Law on Electronic Commerce 2019

PDPA Whistleblower in China

In collaboration with Kingbridge Sun Kuong Law Firm, our PDPA Whistleblower initiative in China aims to strengthen transparency and accountability in data handling practices.

As China continues to advance its data protection framework, this initiative empowers individuals and organizations to report violations confidently and securely, fostering a culture of ethical compliance and legal integrity.

PDPA Whistleblower

THE PEOPLE'S REPUBLIC OF CHINA

What is the primary law governing personal data protection in your jurisdiction? Provide a summary of its Application.

In Mainland China, there are two major legislation that protect personal data, namely Data Security Law (Data Laws) and Personal Information Protection Law (PIPL). PIPL is a new flagship for individual rights in the area of personal information protection, greatly expanding and supplementing the scope of civil laws on personal information rights, such as the Civil Code and the Consumer Protection Law. It grants individual citizens the "right to self-determination" and the "right to know" with respect to their personal information.

The Data Security Law, taking the purpose of implementing the overall concept of national security as its starting point. It balances the risks and benefits of data collection. Article 1 of the Data Security Law establishes the legislative purpose of the Law as follows: "In order to regulate data-processing activities, safeguard data security, promote the development and utilization of data, protect the lawful rights and interests of individuals and organizations, and safeguard the sovereignty, security and development interests of the State, this Law is enacted."

What types of personal information are covered under the PDPA regulations in your country?

According to PIPL article 4, "Personal information" refers to various information **related to an identified or identifiable natural person recorded electronically or by other means, but does not include anonymized information.** Personal information processing includes personal information collection, storage, use, processing, transmission, provision, disclosure and deletion, among others. In this case, PIPL contains multiple elements into the sphere of personal information protection as long as the information could lead to an identifiable person, which means the regulation is considerably strict.

What actions constitute a personal data breach under the PDPA? Additionally, is doxxing considered a criminal offense?

In practice, most data leakage happen when wrongdoers looking for "profits" by commercial use. This phenomenon is very common especially connected with online shopping or financial service. Big data will record your preference and keep sending you with relative promotions. Such leakages were somehow like a grey area of Law, as many applications collect their users' information with their own consent. However, these consents may not be given one hundred percent voluntarily, but as a core condition to keep using these apps. In this sense, regulators should pay more attention to laws that govern in the field of data protection and consumer rights.

On the other hand, illegal access to personal data for criminal use is also common. Scam, espionage and online abuse all connect with data leakage. In terms of doxxing, sadly, most offenders will not face criminal charges unless there is a severe consequence, for example, the victim kills himself.

Author

Ruixiang Zou
Legal Service Management Committee, Deputy Director
zrxac@qq.com

Contact

Kingbridge Sun Kuong Law Firm
Guangdong Province - Guangzhou City Nansha District - Room 401, Building 1, West Zone, Waterfront Plaza, No. 126 Jiaoxi Road
Email: zrxac@qq.com

What measures should businesses take in the event of a personal data breach?

At first, companies should set up comprehensive protocols for collecting users' information and take good care the storage of these information. If data really leaked unfortunately, companies should call the police as soon as they know the leakage. The second step is to evaluate the loss caused by such leakage, and then compensate victims.

What are the penalties for non-compliance with personal data protection laws?

According to Criminal Law of the People's Republic of China article 253. Whoever, in violation of the relevant state regulations, sells or offers personal information of citizens to others, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of not more than 3 years or short-term custody, and concurrently, a fine, or shall be sentenced to a fine only. If the circumstances are especially serious, the offender shall be sentenced to fixed-term imprisonment of not less than 3 years but not more than 7 years, and concurrently, a fine.

Whoever, in violation of the relevant state regulations, sells or offers to others the personal information of citizens which is obtained during his performance of duty or provision of services, shall be given a heavier punishment in accordance with the provisions in the preceding paragraph.

Whoever unlawfully obtains personal information of citizens by stealing or other means shall be punished in accordance with the provisions in the first paragraph.

An entity committing a crime as prescribed in the preceding three paragraphs shall be fined, and the directly responsible persons in charge and other directly responsible persons shall be punished in accordance with the provisions in the corresponding paragraph.

Writer was counseled by a client for defending such an offence, our team searched for a lot of precedents see if we could manage to argue a chance for a sentence of probation. However, no matter what role (accessory or principle) the offenders played they all had to be sent to jail. From this perspective, the punishment for accessing others' protected data is significant.

The KSK Law Firm is a dynamic and rapidly expanding practice delivering comprehensive legal solutions across core sectors such as corporate and commercial affairs, finance and capital markets, intellectual property, real estate and construction projects, public legal affairs, Finance and Taxation. KSK also deals with cross-border legal disputes, and within just four years, KSK has already become the largest local law firm in Nansha.

PDPA Whistleblower in Hong Kong

In partnership with Sun Lawyers LLP, we are advocating for stronger whistleblower safeguards within Hong Kong's evolving Personal Data (Privacy) Ordinance (PDPO). As the city updates its privacy laws to address data breaches, algorithmic decision-making, and consent standards, the absence of dedicated whistleblower legislation remains a critical gap. Our collaboration highlights the urgent need for legal frameworks that protect individuals who report data misuse—ensuring transparency, accountability, and public trust in the digital age.

PDPA Whistle Blower

HONG KONG

What is the primary law governing personal data protection in your jurisdiction? Provide a summary of its Application.

In Hong Kong, the primary law governing personal data protection is the Personal Data (Privacy) Ordinance, Cap 486 (**the "Ordinance"**). This legislation regulates the collection, use, and handling of personal data by both the public and private sectors. The Ordinance aims to safeguard individuals' privacy rights regarding their personal data by establishing clear principles for data handling and granting individuals rights over their information.

A. Data Protection Principles in Hong Kong

The Ordinance mandates that data users comply with six Data Protection Principles (**"DPP"**) outlined in Schedule 1 of the Ordinance:

1) **Purpose and Manner of Collection (DPP1)**: Data must be collected for lawful purposes directly related to a data user's activities. Data subjects should be informed about the necessity of providing their data and the intended use.
2) **Accuracy and Duration of Retention (DPP2)**: Data users must ensure that personal data is accurate and not be kept longer than necessary. If there is doubt about the accuracy of the data, data users should cease using the data immediately.
3) **Use of Personal Data (DPP3)**: Personal data cannot be used for unrelated purposes without the data subject's consent. "Prescribed consent" means the express consent given voluntarily by the data subject.
4) **Data Security (DPP4)**: Data users must take all practicable steps to protect personal data from unauthorized or accidental access, processing, erasure, loss or use by other people without authority.
5) **Information to be generally available (DPP5)**: Data users must publicly disclose the types of personal data they hold, along with their policies and practices for handling that data.
6) **Access to personal data (DPP6)**: A data subject has the right to inquire whether a data user holds any of his personal data and to request a copy of that data. If the data is found to be inaccurate, the data subject may request the data user to correct the record.

What types of personal information are covered under the PDP regulations in your country?

"Personal data" is defined under Section 2 of the Ordinance to mean any data:

A. relating directly or indirectly to a living individual;

B. from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

C. in a form in which access to or processing of the data is practicable.[1]

Examples of personal data include an individual's identity card numbers and fingerprints, which uniquely identify them. Moreover, a combination of details such as telephone numbers, addresses, gender, and age can also be used to identify individuals. It is important to recognize that the cumulative personal information collected by various organizations can further facilitate this identification.

Authors

Fung Kin Wah, Franky
Partner
frankyfung@hksunlawyers.com

Wu Lok Ching, Joycie
Associate
veby.oktia@adcolaw.com

Contact

Sun Lawyers LLP
Unit 02, 21st Floor,
Tower II, Admiralty Centre,
No.18 Harcourt Road,
Hong Kong,
Tel: (852) 2521 6333
Fax: (852) 2524 2724

For example, businesses may track customer purchases to analyze shopping behaviours and tailor promotions to specific segments.

What actions constitute a personal data breach under the PDPA? Additionally, is doxxing considered a criminal offense?

In addition to the Ordinance, the Office of the Privacy Commissioner for Personal Data, Hong Kong (**"Privacy Commissioner"**) has issued various codes of practice and guidance notes in relation to the handling of data breach.

According to the Guidance on Data Breach Handling and Data Breach Notifications (**the "Guidance"**)[2], a data breach is generally regarded as a suspected or actual breach of the security of personal data held by a data user, which exposes the personal data of data subject (s) to the risk of unauthorized or accidental access, processing, erasure, loss or use. Examples include:

- Loss of personal data on devices like laptops or USB drives.
- Improper handling of personal data, such as incorrect disposal or unauthorized database access.
- Data leakage from file-sharing software installations.

Such breaches may violate DPP4, imposing responsibilities on data users.

What measures should businesses take in the event of a personal data breach?

According to the Guidance, businesses should take the following steps in the event of a personal data breach:-

Step 1: Immediate gathering of essential information
As a first step, data users should quickly gather all relevant information of the data breach to evaluate its impact on data subjects and identify suitable mitigation measures.

Step 2: Containing the data breach
Upon detecting the breach and completing an initial assessment, data users should promptly implement measures to contain it as effectively as possible. They should also take remedial actions to minimize potential harm or damage to the affected individuals.

Step 3: Assessing the risk of harm
After gathering all essential information, data users should assess the potential risks of harm to the affected individuals and take appropriate steps to mitigate the impact.

Step 4: Giving data breach notifications
Generally, data users should notify the Privacy Commissioner and the affected data subjects as soon as practicable after becoming aware of the breach, especially if it poses a real risk of harm to those individuals.

When deciding whether to report a breach, data users should evaluate the potential consequences for the affected individuals, taking into account both the seriousness and likelihood of these impacts. They should also consider the implications of not providing notifications.

Step 5: Documenting the breach
Data users should learn from data breach incidents by conducting a post-breach review and enhancing their personal data handling practices. It is essential to maintain a comprehensive record of the incident, including details of the breach, its effects, and the containment and remedial actions taken. Organizations subject to the laws of other jurisdictions should also consider any mandatory documentation requirements under those regulations.

What are the penalties for non-compliance with personal data protection laws?

Section 64(1) of the Ordinance provides that a person commits a criminal offence if they disclose any personal data of a data subject obtained from a data user without consent, with the intent to gain money or property for themselves or for the benefits of others, or to cause financial loss to the data subject. Those convicted may face a fine of HK$1,000,000 and up to 5 years in prison.

- **Regulation of Doxxing**

The Ordinance was amended to include doxxing provisions that took effect on 8 October 2021, establishing a two-tier structure for new doxxing offences:

A. First-tier offence: A summary offence for disclosing a data subject's personal data without consent, with an intent to cause specified harm or recklessness regarding potential harm. Convicted individuals face a fine of HK$100,000 and up to 2 years in prison.[3]

B. Second-tier offence: On top of the requirements under the "first-tier offence", the person would have committed the "second-tier offence" if the disclosure of personal data has in fact caused specified harm to the data subject or any family member of the data subject. Conviction can lead to a fine of HK$1,000,000 and up to 5 years in prison.[4]

Pursuant to section 64(6) of the Ordinance, "specified harm" consists of four limbs, including:-

1) harassment, molestation, pestering, threat or intimidation to the data subject or any family member of the data subjects (**"that person"**);
2) bodily harm or psychological harm to that person;
3) harm causing that person reasonably to be concerned for that person's safety or well-being; or
4) damage to the property of that person.

Doxxing may also involve additional offences, such as breaching an injunction order, which can result in contempt of court and lead to an immediate custodial sentence upon conviction. Moreover, depending on the circumstances, doxxing may involve criminal intimidation and the offence of "access to a computer with criminal or dishonest intent".

Conclusion

The Personal Data (Privacy) Ordinance (Cap. 486) in Hong Kong establishes a comprehensive framework for protecting personal data, highlighting the importance of safeguarding individuals' privacy rights. With clear definitions, structured data protection principles, and strict regulations on data breaches and doxxing, the Ordinance promotes responsible data handling by both the public and private sectors. As the regulatory landscape continues to evolve, ongoing review and development will be essential for effective personal data management in Hong Kong.

Sun Lawyers LLP is a Hong Kong-based medium-sized law firm that was converted to a limited liability partnership ("LLP") in 2017. Established since 2003, we aim to provide an integrated and comprehensive range of legal services to our international and local clientele.

Whilst we provide a wide range of services covering corporate and family matters, civil and criminal litigations as well as commercial and property transactions, wills and probate, notarization (notary public and China-Appointed attestation), our expanding practice will aim to broaden our scope to include IPO, corporate finance, trust, asset management and cross-border matters, as we see a rising demand in these areas. We are also committed to providing our clients with alternative dispute resolution services, such as in arbitration and mediation, so as to assist them to resolve disputes more cost-effectively and amicably.

[1]Section 2(1) of the Ordinance
[2]Guidance on Data Breach Handling and Data Breach Notifications
https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_note_dbn_e.pdf
[3]Section 64(3A) of the Ordinance
[4]Section 64(3C) of the Ordinance

PDPA Whistleblower in Indonesia

In collaboration with ADCO Law, we are advocating for stronger whistleblower protections within Indonesia's newly enacted Personal Data Protection Law. As the country enters a new era of digital governance, ensuring legal safeguards for individuals who report data misuse is essential to uphold transparency and public trust. Our joint efforts aim to align Indonesia's framework with global standards like the GDPR, while fostering a culture of integrity and responsible data stewardship.

PDPA Whistleblower

INDONESIA

Authors

Alexandra Gerungan
Senior Partner
alexandra.gerungan@adcolaw.com

Veby Oktia Hasibuan
Associate
veby.oktia@adcolaw.com

Mutia Ufara Rahmadani
Legal Writer
mutia.ufara@adcolaw.com

What is the primary law governing personal data protection in your jurisdiction? Provide a summary of its Application.

The primary law governing personal data protection in Indonesia is Law Number 27 of 2022 on Personal Data Protection ("**PDP Law**").

The PDP Law is a dedicated regulation that establishes a legal framework for personal data protection in Indonesia. Enacted in 2022, this law establishes general standards for personal data protection that safeguards constitutional rights in the digital era, ensuring a balance between individual privacy and the broader interests of society, while serving as a foundational guideline for secure and responsible data processing across all sectors.

- **Implementation of the PDP Law**

Currently, the Indonesian government is still in the process of drafting implementing regulations in the form of a Government Regulation (*Peraturan Pemerintah*, "**PP**") to further clarify the technical aspects of enforcing the PDP Law. As a result, while the PDP Law has been officially enacted, certain technical provisions are still awaiting further regulation.

Prior to the enactment of the PDP Law, personal data protection regulations in Indonesia were scattered across multiple sectoral laws, including:

1) Law Number 7 of 1992 on Banking, as revoked and partially amended by Law Number 4 of 2023 on Financial Sector Development and Strengthening;
2) Law Number 8 of 1997 on Corporate Documents;
3) Law Number 36 of 1999 on Telecommunications, as amended by Government Regulation in Lieu of Law Number 2 of 2022 on Job Creation;
4) Law Number 23 of 2006 on Population Administration, as amended by Law Number 24 of 2013;
5) Law Number 11 of 2008 on Electronic Information and Transactions ("**ITE Law**"), as amended by Law Number 1 of 2024;
6) Law Number 36 of 2009 on Health, as revoked and amended by Law Number 17 of 2023 on Health;
7) Law Number 43 of 2009 on Archives;
8) Minister of Communication and Informatics Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems;

With the enactment of the PDP Law, Indonesia now has a more comprehensive and integrated legal framework for personal data protection, consolidating previously fragmented sectoral regulations.

What types of personal information are covered under the PDP regulations in your country?

The PDP Law categorizes personal data into two main types:

NO.	GENERAL PERSONAL DATA	SPECIFIC PERSONAL DATA
1	Full Name	Health Data
2	Gender	Biometric Data
3	Nationality	Genetic Data

Contact

ADCO Law
Setiabudi Building 2, 2nd Floor, Suite 205 C JL. HR Rasuna Said Kav. 62,
Kuningan, Jakarta 12920
Indonesia
Tel: (+62) 21 5290 3034
Email: alvin@adcolaw.com

NO.	GENERAL PERSONAL DATA	SPECIFIC PERSONAL DATA
4	Religion	Criminal Records
5	Marital Status	Child-Related Data
6	Other Data that can Identify an Individual	Financial Data
7		Other Data Regulated under Prevailing Laws

What actions constitute a personal data breach under the PDPA? Additionally, is doxxing considered a criminal offense?

The PDP Law defines a personal data breach as any unlawful act involving the processing, disclosing, or using personal data. Under the PDP Law, any processing of personal data—including collecting, storing, and disclosing—**must be based on a lawful basis, which generally requires specific and explicit consent of the Personal Data Subject**. Without such consent or other lawful justification, these activities are deemed unlawful and may constitute a breach.

The law explicitly prohibits the following actions:

1) **Unlawfully obtaining or collecting personal data** that does not belong to oneself for personal or third-party gain, resulting in harm to the Personal Data Subject.[1]
2) **Unlawfully disclosing personal data** that does not belong to oneself.[2]
3) **Unlawfully using personal data** that does not belong to oneself.[3]
4) **Falsifying personal data or creating fake personal data** for personal or third-party gain, which harms others.[4]

- **Is Doxxing Considered a Criminal Offense in Indonesia?**

Yes, doxxing—which involves publicly sharing an individual's personal data without consent—can be considered a criminal offense under the PDP Law. This practice constitutes unlawful disclosure and use of personal data, which is explicitly prohibited under Article 67(1) of the PDP Law. Any individual who unlawfully obtains or discloses personal data to benefit themselves or others, thereby causing harm to the Personal Data Subject, **may face up to 5 years of imprisonment and/or a fine of up to IDR 5 billion.**

In addition to the PDP Law, Article 26 Paragraph (1) of the ITE Law also stipulates that the use of personal information through electronic media **is contingent upon the owner's consent.** If doxxing is done through a digital platform, the victim **can file a civil lawsuit** for the losses incurred, as stipulated in Article 26 Paragraph (2) of the ITE Law.

What measures should businesses take in the event of a personal data breach?

If a personal data breach occurs, businesses acting as Personal Data Controllers must take the following steps:

A. Written Notification Within 3x24 Hours

1) The Personal Data Controller must formally notify the affected Personal Data Subject and the relevant authority within 3x24 hours of the discovery of the breach.[5] Under the PDP Law, the relevant authority refers to the Personal Data Protection Institution or *Lembaga PDP*. However, as this institution has not yet been formally established, the notification should for now be submitted to the Directorate General of Informatics Application (*Ditjen Aptika*), the Ministry of Communication and Informatics.
2) The notification must include the type of personal data exposed, the time and manner of the breach, and steps taken to address and remediate the breach.[6]

B. Public Communication (If Required)

In certain cases, the Personal Data Controller is also required to **publicly disclose** the data breach, particularly if it poses significant risks to the public.[7]

C. Incident Response and Recovery Measures

1) Identify the cause of the breach and implement mitigation measures to minimize further risks.
2) Strengthen security to prevent future breaches, including enhancing system security protocols and data protection mechanisms.

What are the penalties for non-compliance with personal data protection laws?

Non-compliance with the PDP Law can result in administrative and criminal sanctions, depending on the severity of the violation.

A. Administrative Sanctions

Violations of personal data protection obligations may lead to:[8]

1) Written warnings;
2) Temporary suspension of data processing activities;
3) Deletion or destruction of unlawfully obtained personal data;
4) Administrative fines of up to 2% of the company's annual revenue.

B. Criminal Sanctions for Individuals

For more serious violations, the PDP Law stipulates the following criminal penalties:

1) **Unlawfully obtaining or collecting personal data** → Up to 5 years of imprisonment and/or a fine of up to IDR 5 billion.[9]
2) **Unlawfully disclosing personal data** → Up to 4 years of imprisonment and/or a fine of up to IDR 4 billion.[10]
3) **Unlawfully using personal data** → Up to 5 years of imprisonment and/or a fine of up to IDR 5 billion.[11]

C. Sanctions for Corporations

If a corporate entity commits a data-related violation, liability may be imposed on **executives, decision makers, beneficial owners, or the corporation itself.**[12]

The primary sanction for corporations is a fine, which can be **up to 10 times the maximum fine imposed on individuals.**[13]

Additionally, corporations may face **supplementary sanctions**, including:[14]

1) Seizure of profits or assets derived from the violation
2) Partial or total suspension of business activities
3) Permanent prohibition from engaging in certain activities
4) Closure of the business or certain operational sites
5) Obligation to fulfil neglected responsibilities
6) Compensation payments to affected parties
7) Revocation of business licenses
8) Corporate dissolution

These sanctions highlight the **serious legal consequences for corporations** that fail to comply with personal data protection regulations, emphasizing the need for robust data governance policies.

Navigating Indonesia's Personal Data Protection (PDP) compliance is complex, but at ADCO Law, we make it seamless.

As your trusted partner, we provide comprehensive guidance on regulatory frameworks, ensure smooth compliance, and represent you in litigation when needed. From implementing PDP Governance and incident response strategies to advising on operational adjustments, we help your business stay ahead of evolving laws.

Let us help you meet your PDP obligations with confidence. Contact us today for a consultation.

[1]PDP Law Article 65 Paragraph (1)
[2]PDP Law Article 65 Paragraph (2)
[3]PDP Law Article 65 Paragraph (3)
[4]PDP Law Article 66 Paragraph (1)
[5]PDP Law Article 46 Paragraph (1)
[6]PDP Law Article 46 Paragraph (2)
[7]PDP Law Article 46 Paragraph (3)
[8]Article 57 Paragraph (2) PDP Law
[9]Article 67 Paragraph (1) PDP Law
[10]Article 67 Paragraph (2) PDP Law
[11]Article 67 Paragraph (3) PDP Law
[12]Article 70 Paragraph (1) PDP Law
[13]Article 70 Paragraph (2) and (3) PDP Law
[14]Article 70 Paragraph (4) PDP Law

PDPA Whistleblower in Japan

With Japan's amended Whistleblower Protection Act now in full effect, businesses are mandated to establish internal systems that safeguard individuals who report misconduct.

In collaboration with Gensei Ohama, attorney-at-law of ILAWASIA, we provide expert guidance on integrating whistleblower protections within the framework of Japan's Personal Information Protection Act (APPI). Our approach empowers organizations to foster transparency, ensure compliance, and protect whistleblowers—both domestically and across international operations.

PDPA WhistleBlower

JAPAN

Authors

Gensei Ohama
Attorney-at-law
japandesk@ilawasia.com

What is the primary law governing personal data protection in your jurisdiction? Provide a summary of its Application.

In Japan, the primary legislation governing personal data protection is the Act on the Protection of Personal Information (APPI). This law aims to ensure the proper handling of personal information while balancing its usefulness with the protection of individual rights and interests.

The APPI applies to Personal Information Handling Business Operators, defined as those who utilize personal information databases for business purposes, regardless of whether they are for-profit or non-profit entities

The law establishes rules concerning the collection, retention, management, use, and provision of personal information to third parties, as well as procedures for responding to requests for disclosure. Covered entities are required to implement appropriate management systems and operational practices to ensure compliance.

What types of personal information are covered under the PDP regulations in your country?

In Japan, there are two main categories of personal information covered under the APPI: "**Personal Information**" and "**Sensitive Personal Information**."

A. Personal Information

"Personal Information" refers to information relating to a living individual that can identify a specific person by name, date of birth, or other details.[1]

Examples include: photographs of the individual, name, date of birth, telephone number, etc. In addition, unique identifiers such as DNA and fingerprints also fall under the scope of personal information.

B. Sensitive Personal Information

"Sensitive Personal Information" refers to information that is legally designated as requiring special care in handling to prevent unfair discrimination, prejudice, or other disadvantages.

Examples include: race, beliefs, medical history, criminal record, and disabilities.[2]

What actions constitute a personal data breach under the PDPA? Additionally, is doxxing considered a criminal offense?

A. Under the APPI, a **personal data breach refers to any incident where personal data is** disclosed or leaked outside the organization.

Typical examples include:

1) Sending documents containing personal data to an unintended third party
2) Accidentally sending an email with personal data to the wrong recipient
3) Making personal data accessible on the internet due to system misconfiguration
4) Theft of personal data through unauthorized access or similar malicious activity

Contact

ILAWASIA CO., LTD.
319 Chamchuri Square Building,
Floor 17th, Unit 1702, Phayathai Road,
Pathumwan Sub-district,
Pathumwan District, Bangkok, 10330
Thailand
Tel:+66 (0) 2 048 2534
Email: japandesk@ilawasia.com

Furthermore, Personal Information Handling Business Operators are strictly prohibited from acquiring personal data through fraudulent means or using it in a way that facilitates illegal or unjust activities.

Examples of prohibited conduct include:

Providing personal data to a party suspected of engaging in illegal conduct, despite the risk of enabling such behavior

Aggregating and publishing publicly available personal data (e.g., disclosed through court announcements) online, even when such publication could foreseeably lead to unlawful discrimination

B. Doxxing refers to the act of **collecting and publishing another person's personal information** (such as their name, address, phone number, workplace, or social media account) **on the internet without their consent.** It is typically done with the intent to **harass, threaten, or retaliate,** and poses **serious psychological and physical risks** to the victim.

While **doxxing itself is not explicitly defined as a criminal offense under Japanese law**, certain acts associated with doxxing may fall under existing criminal provisions, such as:

1) **Defamation**, when the disclosure harms an individual's reputation
2) **Insult**, in cases of degrading language or exposure
3) **Intimidation**, when threats accompany the release of information

What measures should businesses take in the event of a personal data breach?

Personal Information Handling Business Operators are required to manage personal data securely to prevent incidents such as data breaches. They must also ensure that employees and contractors comply with appropriate security measures.

If personal data is leaked to external parties due to a violation of these obligations, the business operator must take the following actions:

A. Internal Review by the Business Operator

1) Reporting the incident internally and taking steps to prevent further damage
2) Investigating the facts and identifying the root cause
3) Assessing the scope and impact of the breach
4) Considering and implementing recurrence prevention measures
5) Reporting to the Personal Information Protection Commission (PPC)

B. Reporting to the Personal Information Protection Commission (PPC)

If a data breach falls under or is likely to fall under any of the following categories, reporting to the PPC is mandatory:

1) Leakage of **sensitive personal information**
2) Leakage that may be associated with **fraudulent intent**
3) Leakage that may cause **financial harm**
4) Leakage involving **more than 1,000 records**

- **Required Report Contents**
  i. The report to the PPC must include the following details:
  ii. Overview of the incident
  iii. Types of personal data affected or at risk
  iv. Number of affected individuals
  v. Cause of the breach
  vi. Existence and details of secondary damage or potential risks
  vii. Status of measures taken to notify affected individuals
  viii. Status of public disclosure of the incident
  ix. Preventive measures to avoid recurrence
  x. Other relevant information

- **Reporting Deadlines**

In the event of a personal data breach, businesses must promptly report the incident to the Personal Information Protection Commission (PPC) within the following timeframes:

i. **Initial Report**: Within approximately 3 to 5 days, businesses must report any available information from the required items (1) to (9) listed above.

ii. **Detailed Report**: Within 30 days of the incident (60 days if the breach was committed for fraudulent purposes), businesses must submit a full report covering all required items.

C. Reporting to the Personal Information Protection Commission (PPC)

If a data breach occurs that requires reporting to the PPC, the business operator must **promptly notify the affected individual (data subject)**.

Such notification must be provided **to the extent necessary to protect the rights and interests of the individual** and must be carried out using **reasonable and appropriate methods**, such as **postal mail or email**.

What are the penalties for non-compliance with personal data protection laws?

A. Unauthorized Use of Personal Information

If a business handling personal information, its employee, or a person who used to be that business or employee has provided or misappropriated a personal information database or the equivalent (including a personal information database or the equivalent all or part of which has been reproduced or processed) that they handled in the course of their business for the purpose of seeking their own or a third party's illegal profits, they are subject to imprisonment with work for not more than one year or to a fine of not more than 500,000 yen.

B. False Reporting

The Personal Information Protection Commission (PPC) has the authority to request reports or documents and to conduct on-site inspections when it suspects a violation of the law.
If a business operator submits false information, it may be subject to a fine of up to 500,000 yen.

C. Violation of a Cease-and-Desist Order

If deemed necessary to protect the rights and interests of individuals, the PPC may issue recommendations or orders requiring the business to halt violations and implement corrective measures.
Failure to comply with such an order may result in imprisonment of up to one year or a fine of up to 1,000,000 yen. Additionally, non-compliant businesses may be publicly disclosed by the PPC.

D. Dual Liability Provision

If a violation under (1) or (3) is committed by an employee in the course of corporate business, the employing corporation may be subject to a fine of up to 100 million yen.
If a violation under (2) is committed by an employee in the course of corporate business, the employing corporation may be fined up to 500,000 yen.

At ILAWASIA, we provide expert legal counsel for clients seeking guidance on Japan's Act on the Protection of Personal Information (APPI), whether for operations based in Japan or cross-border compliance. Our team supports incident notifications, regulatory filings, and compliance strategies under both legal frameworks, helping businesses maintain compliance with confidence. Contact us for further consultation.

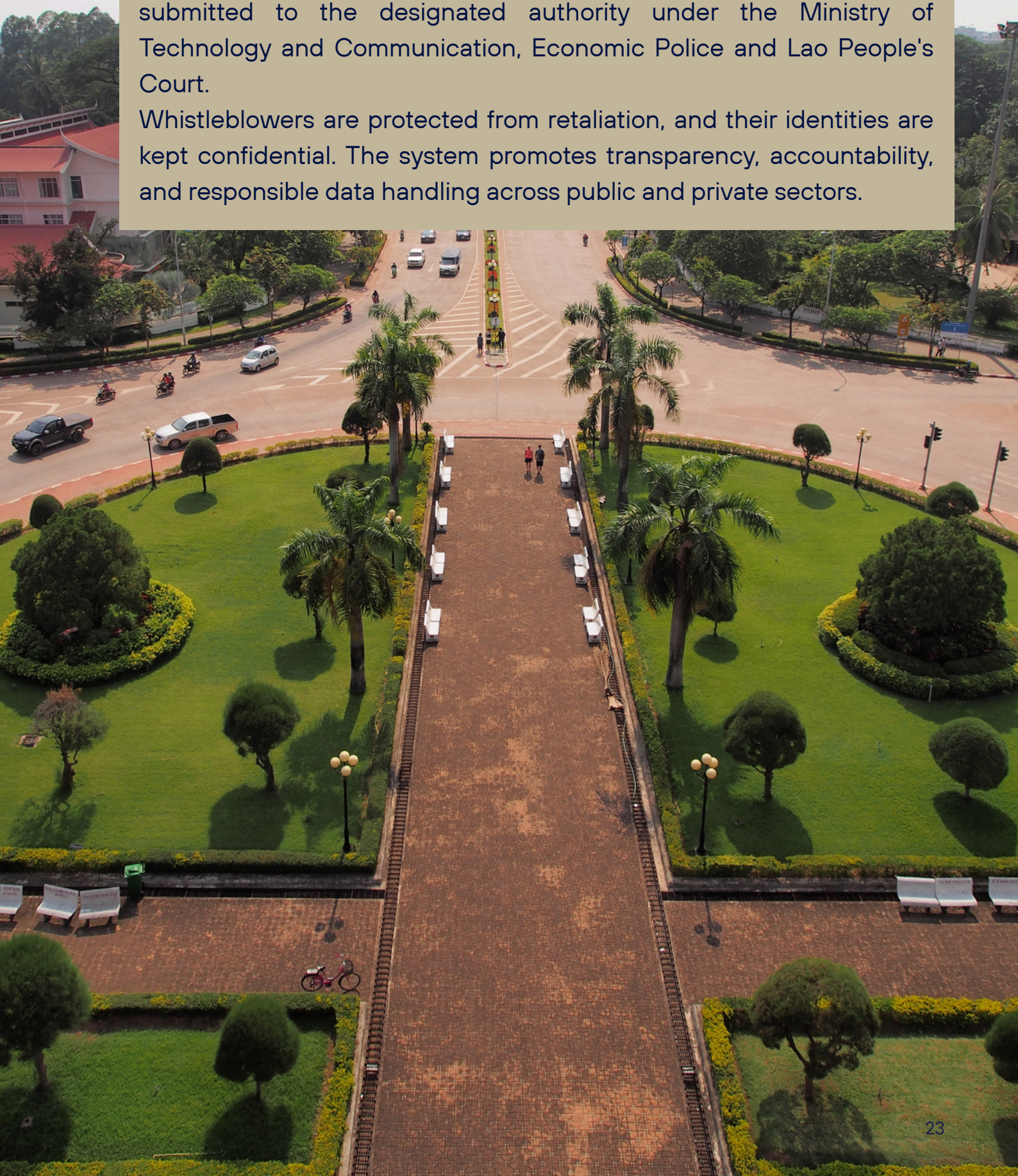
[1]Act on the Protection of Personal Information Article 2, Paragraph 1 and 2, Cabinet Order to Enforce the Act on the Protection of Personal Information Article 1, Enforcement Rules for the Act on the Protection of Personal Information Article 2 to 4
[2]Act on the Protection of Personal Information Article 2, Paragraph 3, Cabinet Order to Enforce the Act on the Protection of Personal Information Article 2, Enforcement Rules for the Act on the Protection of Personal Information Article 5

Remark: This newsletter is not intended to provide legal advice. It is for informational purposes only and should not be considered a substitute for professional legal consultation.

PDPA Whistleblower in Laos

This mechanism empowers individuals to confidentially report violations of personal data protection under Laos' Electronic Data Protection Law 2017 and Law on Penal Code 2017. Reports can be submitted to the designated authority under the Ministry of Technology and Communication, Economic Police and Lao People's Court.

Whistleblowers are protected from retaliation, and their identities are kept confidential. The system promotes transparency, accountability, and responsible data handling across public and private sectors.



PDPA Whistle Blower

LAO PDR

What is the primary law governing personal data protection in your jurisdiction? Provide a summary of its Application.

The primary legal framework governing personal data protection in the Lao PDR is the *Law on Electronic Data Protection No. 25/NA, dated 12 May 2017*. This law applies to individuals, legal entities, and organizations—whether based in Laos or abroad—that conduct business or handle electronic data within the Lao PDR. It establishes key principles and obligations to ensure the security, confidentiality, and lawful use of personal information in both public and private sectors.

In the Lao PDR, personal data protection is governed by a comprehensive framework of 7 (seven) key regulations, each contributing to the legal landscape surrounding data privacy and cybersecurity. These include:

1) Law on Electronic Data Protection (2017)
2) Law on Prevention and Combating Cyber Security Crime
3) Decision on Penalties under the Law on Cyber Crime
4) Law on Electronic Transactions (2023)
5) Penal Code (2017)
6) Instruction on the Implementation of the Cyber Crime Law
7) Instruction on the Implementation of the Law on Electronic Data Protection

Together, these laws and regulations form the foundation for ensuring data privacy, cybersecurity, and legal compliance for individuals, businesses, and organizations operating in Laos.

Under the Law on Electronic Data Protection No. 25/NA, dated 12 May 2017, the term "Personal Data" is defined as electronic data relating to an individual, juristic person, or organization. [1]

The law further defines "Data" as any numbers, letters, or symbols that can be processed by a computer. "Electronic" refers to matters involving the use of technology powered by electricity, including digital processing, magnetic systems, wireless networks, fiber-optic transmissions, electromagnetic systems, or similar methods. Consequently, "Electronic Data" encompasses numbers, letters, moving or still images, audio, video, and other formats stored in digital or electronic form.

This law defines the principles, regulations and measures regarding the management, monitoring, organization, and implementation of electronic data protection, in order to ensure the safe and proper collection, access, use and disclosure of such data. It aims to protect the rights and interests of the State, as well as the rights and legitimate interests of individuals, juristic persons, or organizations, thereby contributing to the nation's economic and social development, ensuring the national, and maintaining peace and order in society.[2]

In the context of Electronic Data Protection, it refers to the use of methods and measures to prevent protected information stored in electronic form from being accessed, used, disclosed, modified, transmitted, transferred or destroyed without permission.[3]

What types of personal information are covered under the PDP regulations in your country?

There are 2 (two) main types of Electronic Data Protection[4] in Lao PDR, 1) General Data and 2) Specific Data. The brief details are as follows:

A. General information: General information refers to the information of individuals, juristic persons or organizations which can be accessed, used and disclosed, but the source of the information must be correctly stated.[5]

Authors

Tanadee Pantumkomon
Partner
Tanadee.P@ilawasia.com

Viphavanh Syharath
Associate
ilawlaos@ilawasia.com

Nisapan Chinnwiicha
Associate
corporate@ilawasia.com

Contact

ILAW LAOS CO., LTD.
Chanthakoummane Road, Unit 7,
Xiang Nguen Village,
Chanthabuly District,
Vientiane Capital, Lao PDR 0100

Tel: (+85620) 99282244

Email: jlawlaos@ilawasia.com

B. Specific information: this type of information is normally recognized as sensitive data.

In this legal context, it refers to a specific information which does not allow individuals, juristic persons, or organizations to access, use or disclose without permission from the owner of the information or the related organizations.

Specific information includes government information and personal information.[6]

For the government information, there must be a security level of information and the procedure for access, use and disclosure in accordance with the laws.[7]

What actions constitute a personal data breach under the PDPA? Additionally, is doxxing considered a criminal offense?

The following actions can be considered as a personal data breach.

1) Access, collect, use, or disclose, destroy, intercept, edit, forge, provide confidential information of the state, an individual, a juristic person or an organization without the permission of the data owner. [8]
2) Transmit or transfer electronic data without the permission of the data owner. [9]

Moving to the action of 'Doxxing' or disclosing confidential information without permission, under the Penal Code, any person who discloses the private information of another that has come to the offender's knowledge in the performance of his/her profession or official duties, thereby causing damage to the other person, shall be sentenced to imprisonment for 3 (three) months to 6 (six) months and a fine from 3,000,000 kip to 10,000,000 kip.

What measures should businesses take in the event of a personal data breach?

There are two scenarios in the event of a personal data breach, first, from a data administrator side, and secondly, from a data owner side.

From a data administrative side, when a personal data breach occurs, there is no mandatory notification under the Law on Electronic Data Protection in Laos. A notification may be made at one's discretion. However, some entities may face special obligation to notify the incident, such as financial service provider (e.g., commercial bank leasing institution), as stipulated in the Law on Commercial Banks in 2023. Furthermore, the bank has the obligation to immediately notify the affected customer of the incident.

Indeed, there is no sanction for a breach of notification obligation to the data administrator. However, please note that there is a sanction related to the disclosure of private and confidential information under the Penal Code as provided in the Answer to Question No. 3 above.

From a data owner, when there is an incident on personal data breach, there are the response measure as follows:[10]

A. Settlement by Compromise[11]

In the event of a dispute concerning electronic data, the parties involved may engage in consultation and reach a peaceful compromise that is mutually beneficial.

B. Administrative Resolution[12]

If the parties cannot reach an agreement or mediation fails, they have the right to submit a request to the Electronic Data Protection Authority for review and resolution.

C. Dispute Resolution by the Economic Dispute Resolution Organization[13]

In the case of an economic dispute arising from electronic data protection activities, the parties have the right to request that the Economic Dispute Resolution Organization to consider and resolve the matter in accordance with the Law on Economic Dispute Resolution.

D. Appeal to the People's Court[14]

In the event of a dispute relating to electronic data protection, the parties have the right to appeal to the People's Court for review and judgment.

E. Resolution of International Disputes[15]

For disputes concerning electronic data protection involving an international element, the relevant laws of the Lao PDR, as well as international treaties and agreements to which the Lao PDR is a party, shall apply.

The enforcing authorities with regard to electronic data protection are the Ministry of Technology and Communications (MTC), the Economic Police and the Lao People's Court.

What are the penalties for non-compliance with personal data protection laws?

- **Penalties under the Law on Electronic Data Protection**[16]

A. Measures against violators include educational and training measures, disciplinary actions, and penalties. Violations of the prohibitions outlined in this legislation (specifically in Articles 31, 32, and 33), which do not constitute criminal offenses, shall be subject to a fine of 15,000,000 kip.[17]

The prohibitions under this legislation mainly fall into three categories (Article 31 to 33):

1) General prohibitions: Unauthorized access, use, disclosure, or manipulation of electronic data are prohibited. This includes spreading harmful content, exploiting system weaknesses, and any actions that violate the law.
2) Data owner: Data owners must not obstruct or tamper with electronic systems, send harmful or false data, exploit system weaknesses, or engage in any unlawful activities.
3) Data controller: Data controllers must not misuse or unlawfully access, use, or disclose personal, sensitive, or confidential electronic information.

B. Individuals, juristic persons, or organizations that violate this law, including the prohibitions set forth in Articles 31, 32 and 33, which do not constitute a criminal offense, will be fined 15,000,000 kip.[18]

- **Penalties under the Penal Code 2017**

1) Any person disclosing the private information of another that has come to the offender's knowledge, in the performance of his/her profession or official duties, and thereby causing damage to the other person, shall be sentenced to imprisonment from 3 (three) months to 6 (six) months and a fine ranging from 3,000,000 kip to 10,000,000 kip.
2) Any person who violates this law and commits a criminal offense shall be punished in accordance with the Penal Code, depending on the severity of the case. The punishment includes imprisonment from 3 (three) months to 5 (five) years, and a fine ranging from 1,000,000 kip to 50,000,000 kip.[19]
3) Any person who, without permission, intercepts, non-public transmissions of computer data by electronic means to, from or within a computer system shall be sentenced to imprisonment for 3 (three) months to 3 (three) years and a fine ranging from 4,000,000 kip to 20,000,000 kip.[20]

At ILAWASIA, we offer expert legal counsel on compliance with the Personal Data Protection Act, including litigation processes for any breach. We assist businesses in navigating their regulatory obligations with confidence. If you need guidance on incident notification, filing complaints, or any other matters related to the Personal Data Protection Act, please contact us for further consultation.

[1]Article 3 - Section 2 - Law on Electronic Data Protection 25/NA, Date 12 MAY 2017
[2]Article 1, Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[3]Article 2, Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[4]Article 8 - Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[5]Article 9 - Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[6]Article 10 - Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[7]Article 10, Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[8]Article 31 (1), Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[9]Article 31 (2), Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[10]Part 8, Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[11]Article 35, Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[12]Article 36, Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[13]Article 37, Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[14]Article 38, Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[15]Article 39, Law o16n Electronic Data Protection No.25/NA, date 12 May 2017.
[16]Article 49, 50, 51, 52, 53 and 54, Law on Electronic Data Protection No.25/NA, date 12 May 2017; and Article 164, 165, 166, 167, 168, 169, 170, 172, 173, 174, Penal Code No. 26/NA, date 17 May 2017.
[17]Article 48 – 54, Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[18]Article 52 - Law on Electronic Data Protection No.25/NA, date 12 May 2017.
[19]Article 164, 165, 166, 167, 168, 170, 171, 172, 173, 177, Penalties under the Penal Code 2017.
[20]Article 167 - Penal Code No. 26/NA, date 17 May 2017.

PDPA Whistleblower in Taiwan

In collaboration with TaipeiLaw Attorneys-at-Law, we explore the intersection of Taiwan's Personal Data Protection Act (PDPA) and the newly enacted Public Interest Whistleblower Protection Act (2025). This landmark legislation empowers individuals to report misconduct involving public and private entities, while ensuring legal safeguards and confidentiality.

Our joint efforts aim to guide organizations in implementing compliant whistleblower systems that uphold data integrity, foster accountability, and align with Taiwan's evolving digital governance landscape.

PDPA Whistleblower

TAIWAN (R.O.C)

What is the primary law governing personal data protection in your jurisdiction? Provide a summary of its Application.

A. Legislative Framework and Scope of Application

The Personal Data Protection Act ("PDPA") of Taiwan was comprehensively amended in 2010 to safeguard individuals' privacy rights and personal dignity, while promoting the reasonable use of personal data.

The PDPA applies to all public and private sector entities that collect, process, or use personal data within Taiwan, or with respect to individuals located in Taiwan.

The National Development Council serves as the central competent authority, with oversight by various sector-specific supervisory agencies.

B. Definition and Categories of Personal Data

Under Article 2 of the PDPA, personal data refers to any information that can directly or indirectly identify an individual, including but not limited to:

1) Basic Identification Data: name, date of birth, national ID number, photograph, registered address.
2) Financial Data: bank account information, credit card details, financial transactions.
3) Health and Medical Data: medical records, health examination results, treatment histories.
4) Social Relationship Data: marital status, family relationships, social networks.
5) Work and Education Data: educational background, employment history, professional qualifications.
6) Sensitive Personal Data: race, political opinions, religious beliefs, health information, and criminal records, which are subject to heightened protection.

What types of personal information are covered under the PDP regulations in your country?

A personal data breach occurs when personal data is subjected to unauthorized access, disclosure, alteration, loss, or destruction, whether through intentional acts or negligence.

Entities that collect, process, or use personal data are legally liable if a breach results from a failure to implement adequate safeguards.

What actions constitute a personal data breach under the PDPA? Additionally, is doxxing considered a criminal offense?

Such liability may involve administrative fines, civil compensation, and, where applicable, criminal penalties.

Doxxing, referring to the disclosure of an individual's personal information without consent, is analyzed under the PDPA and relevant criminal laws:

Authors

Charlies Liu
Managing Partner
Charlies@taipeilaw.com

Contact

TAIPEILAW ATTORNEYS-AT-LAW
17F, No.67, Sec. 2, Dunhua S. Rd.,
Da'an Dist., Taipei City
106, Taiwan (R.O.C.)
Tel:+886-2-2700-6120
Tel:+886-9-3756-9561
Email: master@taipeilaw.com

A. Merely searching publicly available information may not, by itself, constitute an offense.
B. However, the unauthorized collection, disclosure of private information, harassment, or threats may constitute criminal offenses under the Criminal Code and the PDPA.
C. Potential offenses include violations such as infringement of personal privacy, intimidation, and public defamation.

What measures should businesses take in the event of a personal data breach?

Upon discovering a personal data breach, organizations must:

A. Immediately initiate internal investigations and containment measures.
B. Notify affected individuals and relevant competent authorities, generally within 72 hours of becoming aware of the breach.
C. Publicly disclose relevant information when necessary to mitigate damages.
D. Conduct internal reviews and strengthen data protection mechanisms, including staff training and the enhancement of internal procedures.

What are the penalties for non-compliance with personal data protection laws?

A. Civil - Administrative Sanctions: Fines ranging from NT$200,000 to NT$5 million; in serious cases, suspension of data processing or use may be ordered.
B. Civil Liabilities: Application of the presumption of fault principle, requiring data handlers to demonstrate the absence of negligence.
C. Criminal Liabilities: Unlawful processing of sensitive personal data may result in imprisonment of up to five years and/or a fine of up to NT$5 million.

Established in 2008, TaipeiLaw Attorneys-at-Law specializes in finance and investment, corporate governance, intellectual property, labor law, mergers and acquisitions, medical and pharmaceutical law, as well as general practice, and has extensive experience in both litigation and non-litigation legal services. Additionally, we have forged strong partnerships with law firms in Hong Kong, China, Thailand, and the Philippines. With a team of nearly 100 professionals across Taiwan, along with collaborations with overseas law firms, we provide efficient, tailored, and integrated legal services to clients from diverse industries and regions.

PDPA Whistleblower in Thailand

In response to Thailand's evolving data protection landscape, ILAWASIA is proud to lead efforts in promoting whistleblower safeguards within the framework of the Personal Data Protection Act (PDPA). Following the 2025 amendment to the Organic Act on Anti-Corruption, whistleblowers now benefit from enhanced legal immunity and direct support mechanisms—ensuring protection against retaliation for reporting data misuse or breaches.

Our initiative emphasizes the importance of integrating these protections into corporate compliance systems, empowering individuals to speak out with confidence and reinforcing trust in Thailand's digital governance.

PDPA Whistle Blower

THAILAND

What is the primary law governing personal data protection in your jurisdiction? Provide a summary of its Application.

In Thailand, personal data protection is governed by the Personal Data Protection Act B.E. 2562 (2019) (the "**Personal Data Protection Act**"), which has been fully enforced since June 1, 2022. Its purpose is to prevent personal data breaches by setting standards for personal data protection and defining the duties of individuals or business entities involved in the collection, use, or disclosure of personal data (the "**Data Controller**" and "**Data Processor**") under the Personal Data Protection Act.

One key duty of both Data Controllers and Data Processors is to respect the rights of data subjects, including customers, employees, and business partners ("**Data Subject**"). For example, personal data may only be collected, used, or disclosed for the purpose to which the Data Subject has given explicit consent.

In addition, failure to comply with the provisions of the Personal Data Protection Act may result in penalties for both Data Controllers and Data Processors.

What types of personal information are covered under the PDP regulations in your country?

Personal Data means any information that can identify an individual (identify the owner of the information), whether directly or indirectly[1] and personal data can take the form of documents, paper, books, or be stored electronically. It can be divided into 2 types:

1) General Personal Data such as name, address, phone number, photo, etc. as basic personal data.
2) Sensitive Personal Data such as race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal history, health information, disability or mental health information, etc.[2]

However, personal data of deceased persons or information of legal entities such as companies, foundations, associations, organizations are not considered personal information under the Personal Data Protection Act.[3]

What actions constitute a personal data breach under the PDPA? Additionally, is doxxing considered a criminal offense?

With the rise of social media, users often share personal details online, creating vast digital footprints. Unfortunately, this information can be accessed, collected, and redistributed without the Data Subject's consent. Doxxing refers to the malicious act of publicly disclosing a Data Subject's private information, such as their name, address, phone number, or other sensitive details, with the intent to harm, harass, or embarrass them.

Under the Personal Data Protection Act, disclosing sensitive personal data without the Data Subject's explicit consent, or using such data for purposes other than originally intended, is illegal.

This includes the act of doxxing, which is considered a violation of the individual's rights to privacy and security.

Authors

Tanadee Pantumkomon
Partner
Tanadee.P@ilawasia.com

Nannapas Phatcharakeatkanok
Senior Associate
Nannapas.p@ilawasia.com

Wachinorot Siladet
Associate
Wachinorot.S@ilawasia.com

Contact

ILAWASIA CO., LTD.
319 Chamchuri Square Building,
Floor 17th, Unit 1702, Phayathai Road,
Pathumwan Sub-district,
Pathumwan District, Bangkok, 10330
Thailand
Tel:+66 (0) 2 048 2534
Email: info@ilawasia.com

Importantly, doxxing can lead to criminal penalties under the law. If the disclosure of personal data results in harm, damage to the Data Subject's reputation, or causes insult or embarrassment, it is considered a criminal offence.

What measures should businesses take in the event of a personal data breach?

A. Event of a Personal Data Security Measures Breach

Under Section 37(4) of the Personal Data Protection Act, in the event of a breach of personal data security measures that results in the loss, access, use, alteration, modification or disclosure of personal data without authorization, the Data Controller is required to notify the Personal Data Protection Committee ("**PDPC**") of a personal data security measures breach within 72 hours of becoming aware of the incident, and to notify affected Data Subjects if the breach poses a high risk to the rights and freedoms of Data Subjects. The Data Controller must provide a notification with details of the breach and the corrective measures taken ("**Incident Notification**"), unless the breach does not pose a risk to the rights and freedoms of Data Subjects, for example, the personal data is no longer in a usable form because the effective technological measures have been applied. In this case, the data controller is still obligated to submit relevant information, documents, or evidence concerning the incident to the PDPC for consideration as to whether the rights and freedoms of the Data Subject are impacted.

B. Event of Non-Compliance by Data Controller and Data Processor

If Data Controller and Data Processor fails to comply with the provisions of the Personal Data Protection Act, Data Subjects have the right to file a complaint to the Expert Committee under Section 73 of the Act.

The Expert Committee will then assess the complaint to determine its seriousness and issue an order based on the severity. The possible outcomes include:

1) Mediation: If the Expert Committee determines that the complaint can be resolved through mediation, and both parties agree, a mediation process may be initiated.
2) Warning: If the complaint is not considered serious, the Expert Committee may issue a warning to the Data Controller and Data Processor, or require the Data Controller and Data Processor to remedy or resolve the issue, or to cease, suspend, or refrain from the non-compliant action.
3) Administrative Fine: If the complaint is deemed serious, or if the Data Controller and Data Processor fail to comply with a prior warning, the Expert Committee has the authority to impose an administrative fine on the Data Controller and Data Processor.

However, apart from filing a complaint with the Expert Committee above, Data Subject also has the right to file a lawsuit against the Data Controller in court to claim compensation, without needing to file a complaint with the Expert Committee.

What are the penalties for non-compliance with personal data protection laws?

In the event of a personal data breach, the following penalties may apply:

A. Civil Compensation

If the Data Controller and Data Processor fail to comply with the provisions of the Personal Data Protection Act, whether due to intentional actions or negligence, they may be required to compensate the Data Subject for actual damages caused by the breach.[4] In addition, they may be subject to punitive damages of up to twice the actual damages,[5] unless the Data Controller or Data Processor can prove that:

1) The damage was caused by force majeure or resulted from the Data Subject's own actions or omissions.
2) The action was carried out in compliance with an official order issued within lawful authority and duty.

For example, if the court rules that the Data Controller and Data Processor must pay 100,000 Baht in compensation to the Data Subject, the court may order additional punitive damages of up to twice of the actual damages, meaning the total amount payable would be 200,000 Baht.

B. Criminal Penalties

1) If the Data Controller uses or discloses sensitive personal data without the Data Subject's consent or uses the data for purposes other than those originally disclosed, causing harm, damage to reputation, insult, or embarrassment to the Data Subject, they may face imprisonment for up to 6 months, a fine not exceeding 500,000 Baht, or both imprisonment and a fine.[6]

2) If the Data Controller uses or discloses sensitive personal data without the Data Subject's consent or for unauthorized purposes, intending to unlawfully gain benefits for themselves or others, the penalty increases to up to 1 year of imprisonment, a fine of up to 1,000,000 Baht, or both.[7]

In cases where the offender is a legal entity (juristic person), executives, directors, or other persons responsible for the company's operations may be jointly liable with the company. [8]

C. Administrative penalties

The law specifies fines ranging from 500,000 Baht to 5,000,000 Baht, for failure to comply with the Personal Data Protection Act, including:

1) Improper use or disclosure of general personal data.[9]
2) Improper use or disclosure of sensitive personal data.[10]
3) Improper transfer of general personal data abroad.[11]
4) Improper transfer of sensitive personal data abroad.[12]
5) Failure to comply with the Expert Committee's order, provide required explanations, or submit necessary information to the Expert Committee.[13]

Please note that civil compensation, criminal penalties, and administrative penalties are separate and can be imposed independently.

In conclusion, the Personal Data Protection Act establishes crucial mechanisms for addressing personal data breaches and ensuring compliance by Data Controllers and Data Processors. Key obligations include the prompt notification of data breaches to the PDPC within 72 hours and filing complaints in cases of non-compliance. These mechanisms are designed to protect personal data rights and ensure accountability in data processing activities.

At ILAWASIA, we offer expert legal counsel on the Personal Data Protection Act compliance, including litigation process for any breach under the Personal Data Protection Act, assisting businesses in navigating their regulatory obligations with confidence. If you need guidance on incident notification, filing complaints, or any other the Personal Data Protection Act-related matters, please contact us for further consultation.

[1]Personal Data Protection Act Section 6
[2]Personal Data Protection Act Section 26
[3]Personal Data Protection Act Section 6
[4]Personal Data Protection Act Section 77
[5]Personal Data Protection Act Section 78
[6]Personal Data Protection Act Section 79 Paragraph 1
[7]Personal Data Protection Act Section 79 Paragraph 2
[8]Personal Data Protection Act Section 81
[9]Personal Data Protection Act Section 83
[10]Personal Data Protection Act Section 84
[11]Personal Data Protection Act Section 83 and 86
[12]Personal Data Protection Act Section 84 and 87
[13]Personal Data Protection Act Section 89

PDPA Whistleblower in Vietnam

In collaboration with CDLAF Law Firm, we are working to promote stronger whistleblower protections within Vietnam's evolving personal data governance framework. Our joint efforts aim to empower individuals to report data misuse confidently, while helping organizations foster transparency, accountability, and ethical compliance in the digital age.

PDPA Whistle Blower

VIETNAM

What is the primary law governing personal data protection in your jurisdiction? Provide a summary of its Application.

To date, Vietnam has not had a Law/Code to regulate the main field of personal data protection. The main legal regulation to specifically regulate this issue is Decree 13/2023/ND-CP of the Government issued on April 17, 2023 on personal data protection ("Decree 13/2023/ND-CP").

However, the draft Law on Personal Data Protection is in the process of being finalized and is expected to take effect in 2025. When officially passed and effective, this will be the main Law regulating the issue of personal data protection.

♦ **A Summary of Its Application**:

Please refer to a summary of Decree No.13/2023/ND-CP's application below:

A. Subject to Application

This Decree applies to the following agencies, organizations, and individuals directly participating in or related to personal data processing activities in Vietnam:

1) Vietnamese agencies, businesses, and individuals;
2) Foreign agencies, businesses, and individuals in Vietnam;
3) Vietnamese agencies, businesses, and individuals operating abroad;
4) Foreign agencies, businesses, and individuals directly participating in or related to personal data processing activities in Vietnam.

When one of the aforementioned entities participates in or is related to personal data processing activities in Vietnam, specifically performing one or more activities affecting personal data, such as collection, recording, analysis, confirmation, storage, modification, disclosure, combination, access, retrieval, revocation, encryption, decryption, copying, sharing, transmission, provision, transfer, deletion, destruction of personal data, or other related actions, they shall fall under the scope of application of Decree 13/2023/ND-CP and shall be responsible for protecting personal data in accordance with the legal provisions of this Decree.

B. Categories of Protected Personal Data

Personal data shall be classified into two (02) primary categories: Basic Personal Data and Sensitive Personal Data. Detailed information regarding these data categories will be addressed by CDLAF in Section 2, as per your request.

C. Some Key Legal Requirements for Businesses in Personal Data Protection

NO.	LEGAL REQUIREMENTS	TIMELINE
1	**To formulate and promulgate internal regulations/policy** on protection of personal data.	This internal regulation/policy should be made and ready for use as from 1 July 2023, the effective date of Decree 13.
2	To obtain **consent** of personal data owner For example: Client, employee.	**Before** conducting the process of personal data
3	To **make notification** of personal data processing.	**Before** conducting the process of personal data (Notification is made once).
4	To **handle** personal data owner's request	Whenever if requested

Author

Nguyen Thi Hoa
Managing Partner
hoa.nguyen@cdlaf.vn

Contact

CDLAF Law Firm
Room 7.01, TMS Building, 172 Hai Ba Trung St., Da Kao Ward, D1, HCMC, Vietnam
Tel: (+84) 909 668 216
Email: info@cdlaf.vn

NO.	LEGAL REQUIREMENTS	TIMELINE
5	To **appoint/assign** specialized internal department and personnel	Before processing **sensitive** personal data
6	To **make a dossier** in writing for impact assessment of personal data processing	From the commencement date of personal data processing
6.1	To **submit** 01 original copy of such dossier to the MPS and **notify** MPS in writing of any amendment thereof (if any)	Within **60 days** after **processing** data
7	To **make a dossier** in writing for impact assessment of personal data transferring abroad	From the commencement date of personal data processing
7.1	To **submit** 01 original copy of such dossier to the MPS and **notify** MPS in writing of any amendment thereof (if any)	Within **60 days** after **processing** data.
8	To **notify/report** MPS of breach of personal data protection	Within 72 hours of the breath occurring (if later than 72 hours, an explanation of reason for delay is required)
8.1	To **make a written confirmation** of the violation against regulations on protection of personal data	When violation happens
8.2	To **cooperate with MPS** in handling such violation.	Upon requested
9	To **record and store** log of the processing of personal data	

D. Rights of Data Subjects

A data subject is an individual whose personal data is reflected.

Data subjects possess the following rights: the right to be informed; the right to consent; the right to access (to view, amend, or request amendment of their personal data); the right to withdraw consent; the right to erasure of data; the right to restrict data processing; the right to object to data processing; the right to complain, denounce, or initiate legal proceedings; the right to claim compensation for damages; and the right to self-protection. Enterprises involved in personal data processing activities are required to ensure the rights of data subjects.

What types of personal information are covered under the PDPA regulations in your country?

Personal data, as stipulated in Decree 13/2023/ND-CP, is categorized into two (02) types, including: Basic Personal Data and Sensitive Personal Data. Specifically:

A. *Basic Personal Data* Encompasses:

1) Full name, including middle name (s) and any aliases (if any);
2) DOB; date of death or declaration of missing status;
3) Gender;
4) Place of birth, place of birth registration, permanent residence, temporary residence, current residence, native village, contact address;
5) Nationality;
6) Image of the individual;
7) Telephone number, national identity card number, personal identification number, passport number, driver's license number, vehicle license plate number, personal tax identification number, social insurance number, health insurance card number;
8) Marital status;
9) Information concerning family relationships (parents, children)
10) Information pertaining to the individual's digital accounts; personal data reflecting activity and activity history in cyberspace;
11) Other information associated with or enabling the identification of a specific person, excluding sensitive personal data.

B. *Sensitive personal data* refers to personal data associated with an individual's privacy, the infringement of which would directly impact the individual's legitimate rights and interests, including:

1) Political opinions, religious beliefs;
2) Health status and private life recorded in medical records, excluding blood type information;
3) Information related to racial or ethnic origin;
4) Information concerning an individual's inherited or acquired genetic characteristics;

5) Information regarding an individual's unique physical attributes or biological characteristics;
6) Information concerning an individual's sexual life or sexual orientation;
7) Data on crimes or criminal offenses collected and stored by law enforcement agencies;
8) Customer information of credit institutions, foreign bank branches, payment intermediary service providers, and other authorized organizations, including customer identification information as prescribed by law, account information, deposit information, asset deposit information, transaction information, and information about organizations or individuals acting as guarantors at credit institutions, bank branches, or payment intermediary service providers;
9) Data on an individual's location determined through location services;
10) Other personal data prescribed by law as unique and requiring necessary security measures.

What actions constitute a personal data breach under the PDPA? Additionally, is doxxing considered a criminal offense?

According to Decree 13, the following prohibited acts regarding personal data can be summarized as follows:

1) Unauthorized collection and processing of data: collecting or processing data without the consent of the data subject or contrary to the committed purpose.
2) Unauthorized disclosure, sharing, or dissemination of personal data.
3) Infringement of the rights of the data subject
4) Failure to ensure data safety and security
5) Processing and transferring data abroad in violation of legal regulations.
6) Using personal data for illegal purposes

We understand that doxxing involves the use of sensitive or confidential information, statements, or records to harass, expose, cause financial harm, or otherwise exploit targeted individuals. If doxxing activities fulfil the elements of related criminal offenses, such as: Violating the confidentiality or security of another person's correspondence, telephone, telegraph, or other forms of private communication; Crime of extortion, etc., as stipulated by criminal law, they may be considered criminal offense.

What measures should businesses take in the event of a personal data breach?

In accordance with the legal provisions stipulated in Decree 13/2023/ND-CP, in the event of detecting a violation of personal data protection regulations, enterprises processing personal data are required to notify the Ministry of Public Security (Cybersecurity and High-Tech Crime Prevention Department) within 72 hours of the occurrence of the violation.

Additionally, enterprises must compile a Record of Confirmation regarding the occurrence of the violation of personal data protection regulations and cooperate with the Ministry of Public Security (Cybersecurity and High-Tech Crime Prevention Department) in handling the violation.

However, the notification and cooperation with the Ministry of Public Security for handling violations are only applicable after a violation has occurred. Therefore, to prevent violations and minimize potential damages in the event of a personal data breach, enterprises should proactively develop and implement management and technical measures to protect data.

What are the penalties for non-compliance with personal data protection laws?

As mentioned, depending on the severity of the personal data protection violation, the penalty can be administrative sanctions or criminal prosecution. However, there are currently no specific regulations on penalty amounts. In the near future, when the Law on Personal Data Protection is officially enacted, detailed regulations on penalty amounts may be applied.

At CDLAF Law Firm, we provide specialized legal services in personal data protection law and cyber information security. In addition, we offer legal consultancy on cybersecurity and personal data protection—particularly with respect to the processing and cross-border transfer of personal data. With a team of reputable and experienced lawyers, CDLAF offers legal representation and protects clients' rights and interests in disputes related to personal data and cybersecurity in court proceedings and commercial arbitration.

With the goal of minimizing legal risks and building consumer trust in the digital environment, CDLAF is committed to accompanying businesses through every stage—from preparation and implementation of personal data protection.

Participating Offices

CAMBODIA - PHNOM PENH
ILAW Cambodia Law Office
89A, Level 1, St.294, Phum 3, Sangkat Boeung Keng Kan I, Khan Boeung Keng Kang, Phnom Penh, Cambodia

CHINA - GUANGZHOU
Kingbridge Sun Kuong Law Firm
Guangdong Province - Guangzhou City Nansha District - Room 401, Building 1, West Zone, Waterfront Plaza, No. 126 Jiaoxi Road, China

HONGKONG
Sun Lawyers LLP
Unit 02, 21st Floor, Tower II, Admiralty Centre, No.18 Harcourt Road, Hong Kong,

INDONESIA - JAKARTA
ADCO Law
Setiabudi Building 2, 2nd Floor, Suite 205 C JL. HR Rasuna Said Kav. 62, Kuningan, Jakarta 12920, Indonesia

JAPAN
ILAWASIA Co., Ltd.
319 Chamchuri Square Building, Floor 17th, Unit 1702, Phayathai Road, Pathumwan Sub-district, Pathumwan District, Bangkok, 10330 Thailand

LAOS - VIENTIANE
ILAW LAOS Co., Ltd.
Chanthakoummane Road, Unit 7, Xiang Nguen Village, Chanthabuly District, Vientiane Capital, Lao PDR 0100

TAIWAN - TAIPEI
TaipeiLaw Attorneys-at-Law
17F, No.67, Sec. 2, Dunhua S. Rd., Da'an Dist., Taipei City 106, Taiwan (R.O.C.)

THAILAND - BANGKOK
ILAWASIA Co., Ltd.
319 Chamchuri Square Building, Floor 17th, Unit 1702, Phayathai Road, Pathumwan Sub-district, Pathumwan District, Bangkok, 10330 Thailand

VIETNAM - HO CHI MINH CITY
CDLAF Law Firm
Room 7.01, TMS Building, 172 Hai Ba Trung St., Da Kao Ward, D1, HCMC, Vietnam

DISCLAIMER

The handbook is intended for general informational purposes only and should not be interpreted as legal advice by ILAW Cambodia Law Office, Kingbridge Sun Kuong Law Firm, Sun Lawyers LLP, ADCO Law, ILAWASIA, ILAW Laos, Taipeilaw Attorneys-at-Law, and CDLAF Law Firm.

The viewpoints expressed herein do not represent the official legal stance of any of these firms. Consequently, the firms cannot be held accountable for any actions taken by individuals who use this article for purposes other than those for which it is intended.