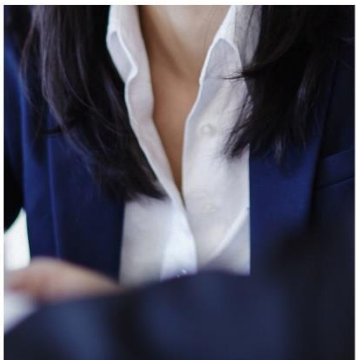
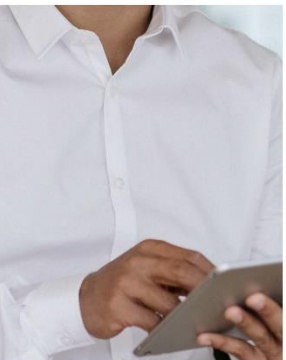
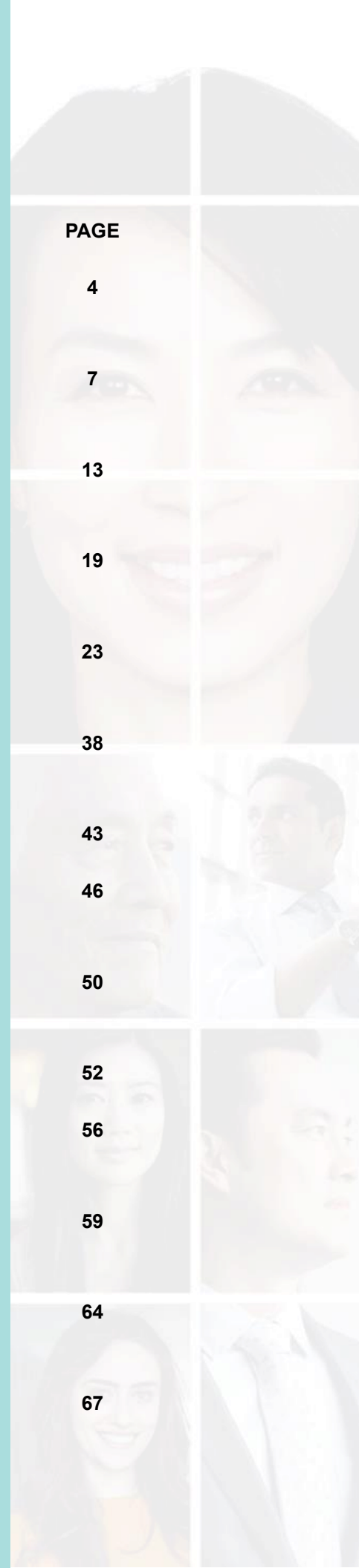


# ASEAN ROUNDUP



# CONTENTS

NO.	COUNTRY	CONTENT	PAGE
1.	Singapore	Report of the Committee to Enhance Singapore's Corporate Restructuring and Insolvency Regime	4
2.	Singapore	DrewTech Series (Chapter 16): Speak, Friend and Enter – Access Controls and Authorised Users	7
3.	Indonesia	DANANTARA: Indonesia's New Sovereign Wealth Fund Marks a New Era for State-Owned Enterprises	13
4.	Malaysia	How A Confusion Clause Shapes Jurisdiction Battles — Arbitration or Court?	19
5.	Philippines	Legal Environment of Data Protection in the Philippines	23
6.	Cambodia	Funding Cuts and Mass Layoffs Due to Financial Stress in Cambodia	38
7.	Laos	New Regulations on Foreign Currency in Laos	43
8.	Laos	Laos' New Regulation on Biopharmaceuticals, Gene Therapy, and Stem Cells	46
9.	Myanmar	Myanmar Changes Documentation Rules for Share Transfers and Director Appointments	50
10.	Myanmar	Myanmar Issues Cybersecurity Law	52
11.	Thailand	Thailand Amends Emergency Decree on Technology Crime	56
12.	Thailand	The Intellectual Property Implications of Thailand's Entertainment Complex Bill	59
13.	Vietnam	Vietnam's Government Restructuring: Key Changes and Implications for Businesses	64
14.	Vietnam	A Closer Look at Vietnam's Decree 147 on Internet Services and Online Information	67





# SINGAPORE

DREW & NAPIER LLC

## Restructuring & Insolvency Legal update

# Report of the Committee to Enhance Singapore's Corporate Restructuring and Insolvency Regime

## **Recommendations for Singapore's Restructuring and Insolvency Framework**

The Committee's report sets out recommendations broadly categorised as follows:

- a) strengthening the judicial management regime;
- b) refining the cross-class cramdown in schemes of arrangement;
- c) refining the framework and tools for efficient debt restructurings; and
- d) adopting the UNCITRAL Model Laws relating to insolvency.

The recommendations are summarised under the respective category headings below.

### **Strengthening The Judicial Management Regime**

The Committee noted that the value proposition of the judicial management regime is being eroded by its divergent purposes (i.e. having both restructuring and recovery functions). The Committee recommended that judicial management should be reconceptualised to emphasise its restructuring functions, and that both creditors and debtors should continue to have standing to apply to court to place the debtor in judicial management. The Committee also recommended that the judicial manager should continue having the ability to pursue clawback actions in the reconceptualised regime. As for the judicial manager's remuneration, the Committee recommended for it to be based on a model that allows flexibility to better align such remuneration with successful outcomes in judicial management proceedings (in particular, by including a "success fee" component).

### **Refining The Cross-Class Cramdown in Schemes of Arrangement**

Cross-class cramdowns currently require a majority in number and 75% in value of creditors across all classes to approve the scheme. The Committee recommended removing these requirements to make cramdowns more functional. The Committee also recommended expanding the scope of cross-class cramdowns to encompass shareholders in appropriate circumstances, reflecting the economic reality of the debtor's capital structure in a financially distressed situation.

### **Refining The Framework and Tools for Efficient Debt Restructurings**

Shareholder approval is currently required for a company to dispose of all or substantially all of its property or to issue new shares. The Committee

recommended streamlining the process for disposing the company's property and issuing new shares in a judicial management or scheme of arrangement, which may otherwise create uncertainty on an agreed restructuring plan among creditors. The Committee also recommended providing the court with the discretion to assess and appoint neutral third-party individuals as restructuring officers. Such individuals may perform a range of roles (e.g. to act as a monitor and provide business expertise) to assist with a restructuring under a scheme of arrangement.

### **Adopting the UNCITRAL Model Laws Relating to Insolvency**

The Committee recommended that two UNCITRAL Model Laws (Enterprise Group Insolvency, and Recognition and Enforcement of Insolvency-Related Judgments) be implemented in Singapore. This would further strengthen Singapore's ability to deal with international, cross-border restructuring and insolvency matters.

The report may be accessed [here](#). The Ministry of Law has also issued a [press release](#) on its website. If you have any queries on the recommendations, please feel free to contact us.

*The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances. Copyright in this publication is owned by Drew & Napier LLC. This publication may not be reproduced or transmitted in any form or by any means, in whole or in part, without prior written approval*

---

## CONTACTS



### Mohan Gopalan

Director, Corporate  
Restructuring &  
Workouts  
Drew & Napier LLC

**T:** +65 6531 2755  
**E:** mohan.gopalan  
@drewnapier.com



### Teri Cheng

Director, Corporate  
Restructuring &  
Workouts  
Drew & Napier LLC

**T:** +65 6531 2456  
**E:** teri.cheng  
@drewnapier.com



### Erica Phoon

Senior Associate,  
Corporate Restructuring  
& Workouts  
Drew & Napier LLC

**T:** +65 6531 2291  
**E:** erica.phoon  
@drewnapier.com

## DrewTech Series (Chapter 16): Speak, Friend and Enter – Access Controls and Authorised Users

### Introduction

A key element in any security system is ensuring that only persons who should have access to something (whether it be physical premises or data) are able to obtain access to that thing. Beyond common business sense, it is important that organisations comply with this since there are legal implications for failing to do so. Unauthorised access to personal data can amount to a data breach, attracting increased regulatory scrutiny and the imposition of penalties. Confidentiality agreements will typically require that confidential information is only disclosed within an organisation to those individuals who need to have access to that information. It therefore should be apparent that ensuring proper access controls is imperative for any organisation.

However, what would amount to proper access controls? Turning back to the examples cited above, the Personal Data Protection Act 2012 states that an organisation *must “protect personal data in its possession or under its control by making reasonable security arrangements...”*. Confidentiality agreements may typically state that *“Recipient shall protect the Confidential Information in its possession with not less than a reasonable standard of care”*. The precise technical steps are not specified. This is all well and good for lawyers and regulators since it gives flexibility in ensuring that the legal protections keep up with changing technological trends; not so good for organisations who actually need to implement the protections.

In the hope of shedding some light on the issue, this article explores three strategies commonly employed by organisations, and how they have been treated in the realm of the law

### Passwords

The idea of using passwords to protect access is ancient. The concept is simple – only authorised persons know a secret, knowledge of which confirms that the person seeking access is authorised.

However, the development of technology means that the passwords that must be used become increasingly complex and convoluted. Modern software developed with the specific objective of cracking passwords can try a myriad possible passwords within fractions of a second – one company boasts that their password cracking engine can try 1.4 trillion guesses per second. Using a pure “brute-force” approach, they claim that they will be able to guess every possible password permutation between 1 to 8 characters within an hour. Building on pure computational power, another commonly employed approach is to apply some sophistication and use a “dictionary attack”. Relying on the tendency of humans to use common words as passwords, the password cracking software tries passwords which are known to be popular. A list of the top 10,000 most popular passwords can be easily found online – if your password is in this list, you should change it immediately.

What then are the legal frameworks or guidance from authorities regarding passwords? We address a few of these below.

It is a consistent theme across the decisions and guidance published by the Personal Data Protection Commission (**PDPC**) that they consider the use of high-quality passwords to be important. The following insights may be gleaned:

- a) Passwords should have complexity and length requirements. In what is a likely nod to changing technological practices and an evolving threat environment, recommendations on the specific length and level of complexity are not fixed. An earlier 2017 publication suggested that the password should be at least 8 characters long and contain at least 1 alphabetical character and 1 numeric character. A later 2021 decision has recommended a passphrase such as *"Iwant2l@se10kg"* (read: *"I want to lose 10kg"*), which is 14 characters and also includes symbols and both upper and lower-case alphabets.
- b) However, the complexity and length requirements above cannot simply be enforced by configuring the software to accept only passwords of minimum length and complexity. The reason for this is apparent – employees may use passwords that comply with the rules in form, but are in practice easy to guess (e.g., *Pa\$\$w0rd*). Multiple organisations have been sanctioned by the PDPC in circumstances where there were passwords which included the organisations' name. It may therefore be suggested that the software should, if possible, also contain a blacklist of words that cannot be used as part of a password.
- c) Building on the foregoing point, a written password policy is required. The PDPC has specifically expressed that it is not sufficient to enforce password requirements through technical measures. The PDPC has also specifically noted that technical policies *"alone may not ensure that users refrain from incorporating easily-guessable words or phrases such as their username, real name, birth date, or the organisation's name in the password"*. Organisations have been sanctioned for failing to (amongst other things) impress on their employees the importance of password security.

The foregoing recommendations are not exhaustive. The unfortunate truth is that legitimate organisations are locked in an arms race against threat actors (see our previous legal update *Red Queen Races – Vulnerability Disclosure Programs*), and the recommendations on password security have constantly evolved. The Singapore Cyber Security Agency recommended in 2022 that passwords should contain *"at least 12 characters comprising upper-case and lower-case letters, numbers and/or special characters"*. In 2024, the PDPC reiterated this recommendation in a decision. However, 2024 recommendations by the United States National Institute of Standards and Technology suggest that complexity requirements may in fact be counterproductive – they cause user frustration and create passwords that are in form compliant but in practice barely more secure:

*"a user who might have chosen "password" as their password would be relatively likely to choose "Password1" if required to include an uppercase letter and a number or "Password1!" if a symbol is also required."*

### **Multi-Factor Authentication**

Multi-factor authentication (“**MFA**”) aims to address some of the weakness of passwords mentioned above. The concept is simple – if one secret is compromised, the attacker will still need to know a second secret (or even greater number of secrets) to gain access to the system.

The technical implementation of MFA varies widely. There are phone-based applications which generate a one-time password which must be entered together with the account password. There are hardware tokens which must be physically plugged into a device to confirm that the user is who they claim to be. The basic underlying theory is the same, that the attacker must not only compromise the account password but also gain access to a piece of physical hardware. This is a simplification of the process – there are various exploits in the wild which can under various circumstances bypass this security mechanism without physical possession of the authentication device but are beyond the scope of this article.

The PDPC has, since at least 2022, taken the view that MFA is now a baseline standard, at least for accounts with administrative privileges. Failure to implement MFA can on its face amount to a breach of the obligation to protect personal data. Since then, there have been a significant number of decisions by the PDPC which mention a failure to implement MFA, indicative perhaps of the growing importance of this security measure.

In our experience, this requirement is sometimes difficult to accept for some organisations, who use older legacy systems which due to technical limitations may not be able to implement MFA. To this end, it is difficult to definitively state when it would be acceptable to not have 6 MFA implemented. The PDPC has made the following pronouncements which may be instructive:

- a) As mentioned above, the PDPC has commented that not having MFA can amount to a breach of the data protection obligation, but this subject to the caveat that an organisation can show that *“its omission is reasonable or implementation of [MFA] is disproportionate”*;
- b) However, the PDPC also notes that as MFA becomes more readily available at a lower cost, the expectation to implement MFA will also rise; and
- c) The PDPC has sanctioned organisations for (amongst other things) using outdated and unpatched software with known vulnerabilities where updates are available.

Synthesising the above, an organisation not implementing MFA because of a legacy system may need to be prepared to explain:

- a) why usage of that legacy system is required (e.g., because no newer version is available); or
- b) that the legacy system without MFA capabilities does not have access to sensitive data.

### **Access Control Privileges**

Another strategy commonly employed is that of access control privileges. The concept is straightforward – individuals in an organisation should only be able to access information that they need to know to perform their roles within that organisation.

In practice, what this would mean is that an organisation must consider the various roles and responsibilities of its different departments (as well as the ranks of the individuals in these departments) and determine how much access to the information in the organisation each group of individuals should have. For instance:

- a) The human resources department could require access to information about employees to perform functions such as managing payroll, but they would not typically require information about confidential sales deals that are being brokered;
- b) The marketing department may require information about customer profiles to target advertisements or advertising campaigns, but may only need limited information about technical details of new, secret products still in development; and
- c) System administrators may require administrator accounts with a high level of access to the entire organisation's IT infrastructure to troubleshoot and resolve issues. These "master keys" should be 7 jealously guarded, and individuals should have their access revoked once they leave the organisation.

The legal importance of such controls cannot be understated. We set out below a selection of actual examples where failure of access control privileges resulted in serious consequences:

- a) In one instance, an organisation failed to revoke login credentials of an administrator account belonging to an ex-employee. It transpired that an attacker hacked the ex-employee's personal laptop, obtained the credentials, and accessed the organisation's IT system. Result: a pornographic picture was uploaded on the organisation's customer-facing mobile application and personal data of customers was exfiltrated from the organisation and offered for sale.
- b) In another instance, an organisation stored personal data of its employees (e.g., names, bank account information, salary information) on unsecured shared drives. It also allowed all its employees to install and uninstall applications on their laptops. It transpired that an attacker was able to access the company servers, potentially because an employee had downloaded unlicensed software and removed existing software protections. Result: 81.95GB of data was exfiltrated and posted online, affecting 5,640 individuals.

### **Conclusion**

Ensuring robust access controls is paramount for any organisation to safeguard sensitive information and comply with legal requirements. The strategies discussed – password complexity, MFA, and access control privileges – are essential components of a comprehensive security framework. By adopting these strategies and staying informed about evolving security recommendations, organisations can better protect their data and mitigate legal risks.

*The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances. Copyright in this publication is owned by Drew & Napier LLC. This publication may not be reproduced or transmitted in any form or by any means, in whole or in part, without prior written approval*

---

## **CONTACT**



### **Rakesh Kirpalani**

Director, Dispute  
Resolution &  
Information Technology  
Drew & Napier LLC

**T:** +65 6531 2521

**E:** rakesh.kirpalani  
@drewnapier.com



# INDONESIA

MAKARIM & TAIRA S.

## DANANTARA: Indonesia's New Sovereign Wealth Fund Marks a New Era for State-Owned Enterprises

Indonesia has launched a new sovereign wealth fund that will take charge of key state-owned enterprises (“**SOEs**”), with the aim of maximizing dividends, increasing investment opportunities, and attracting global investors, while seeking to assuage concerns over potential political interference.

The **Danantara Investment Management Agency (*Lembaga Pengelola Investasi Daya Anagata Nusantara*)** was created under the Third Amendment to Law No. 19 of 2003 on State-Owned Enterprises (“**Amended SOE Law**”), which was approved by Indonesia’s House of Representatives on 4 February 2025 and enacted on 24 February 2025 as Law No. 1 of 2025 along with the enactment of Government Regulation No. 10 of 2025 on the Organization and Governance of Daya Anagata Nusantara Investment Management Agency.

The term **Danantara** is intended to reflect economic strength as the energy for Indonesia’s future, as **Daya** means energy or strength, **Anagata** means future and **Nusantara** means the Indonesian homeland.

Danantara, which will serve some functions similar to Singapore’s Temasek Holdings, will act as a ‘super-holding’ and manage seven SOEs in its initial stage:

- a) PT Pertamina – state oil and gas company;
- b) PT Mineral Industri Indonesia (MIND ID) – Indonesia’s mining industry holding company;
- c) PT PLN – state electricity company;
- d) PT Telkom Indonesia Tbk – state telecommunications company;
- e) PT Bank Rakyat Indonesia (BRI) – state-owned bank focused on microfinance and small to medium-sized businesses;
- f) PT Bank Negara Indonesia Tbk (BNI) – state-owned commercial bank; and
- g) PT Bank Mandiri Tbk – Indonesia’s largest state-owned bank by assets.

Danantara is also expected to consolidate Indonesia’s existing sovereign wealth fund, the Indonesia Investment Authority (“**INA**”). It will manage assets totaling IDR 9,049 trillion (around USD 571.6 billion), surpassing the minimum capital requirement of at least IDR 1,000 trillion specified in the Amended SOE Law.

President Prabowo Subianto has confirmed that an initial fund of USD 20 billion will be reallocated to Danantara from his budget cuts across ministries and agencies as part of his austerity measures. Danantara will invest in Indonesia’s natural resources and assets to support sustainable and high-impact projects in renewable energy, advanced manufacturing, downstream industries, food production, and food security.

Minister of SOEs, Erick Thohir has described Danantara as a vehicle to consolidate SOE assets and investments, representing the President's vision for SOEs to generate their own funding instead of relying on the state budget, while their profits accelerate investment and economic growth.

Danantara marks a major shift in how SOEs are managed by centralizing assets under a single holding. Its establishment will also affect Indonesia's sovereign wealth structure and broader economic strategy.

### **Danantara's Role and Presidential Oversight**

The Amended SOE Law has restructured the governance of SOEs, separating operational and regulatory functions. Under the new framework, the Ministry of SOEs functions as a policymaker and supervisor, while Danantara will serve as the operator and manager. Danantara will report directly to the President, ensuring checks and balances.

Danantara has three governing bodies: a Supervisory Board, Managing Board, and Advisory Board. Members of these bodies are appointed and terminated solely at the President's discretion. Their appointments have been formalized through Presidential Decree No. 30 of 2025 on the Appointment of Danantara's Supervisory Board and Managing Board. The details are as follows:

- a) **Supervisory Board:** Oversees Danantara's operations, ensuring compliance and effective management. It is chaired by the Minister of SOEs, currently Erick Thohir, alongside a Ministry of Finance representative and an appointed state official. Members serve five-year terms, with a one-time reappointment option.
- b) **Managing Board:** Handles Danantara's daily operations and investment strategies. It consists of professionals, with one serving as the agency head. Members serve five-year terms, with a one-time reappointment option. The board will also form an investment and risk management committee by resolution.
- c) **Advisory Board:** Provides advice to Danantara and consists of one chairperson and additional members.

The Head of Presidential Communications has confirmed that along with Erick Thohir, Muliaman Hadad will become the Vice Chairman of the Supervisory Board, Rosan Roeslani (current Minister of Investment and Downstream Industry) will become the Head of Danantara and former President(s) of the Republic of Indonesia will serve as the Advisory Board.

The Amended SOE Law also adopts the business judgement rule, which **protects the Minister of SOEs, Danantara's boards, and staff from legal liability for investment losses** if they can prove that:

- a) The losses were not due to their fault or negligence;
- b) They have acted in good faith and with due diligence in accordance with investment objectives and governance principles;

- c) They had no direct or indirect conflicts of interest in the investment management actions; and
- d) They did not unlawfully obtain personal gain.

### **Key Updates**

#### **a) Holding Companies**

Danantara will invest directly or through:

1. **Investment Holding:** Focused on asset management and optimizing investment value;
2. **Operational Holding:** Responsible for managing SOE operations to improve efficiency; and
3. **Third parties.**

The Minister of SOEs and Danantara will establish the Investment Holding and Operational Holding to ensure a structured and efficient approach to managing state assets.

Both holding companies will operate under Danantara's oversight and maintain alignment with the agency's broader economic objectives. Each will be structured as a limited liability company with its own board of directors and commissioners. Ownership will be divided as follows:

Share Classification	Share Percentage	Ownership	Remarks
Dwiwarna A Series	1%	The Republic of Indonesia	Special/preferential rights through Ministry of SOEs
B Series	99%	Danantara	N/A

The Head of Presidential Communications has also confirmed that Pandu Sjahrir will become the Chief Investment Officer while the Vice Minister of SOEs, Dony Oskaria will become the Chief Operating Officer.

#### **b) Audits**

Concerns have been raised about Danantara's transparency, given the scale of assets being managed. To address this, the Amended SOE Law provides that the State Audit Board (*Badan Pemeriksa Keuangan – BPK*) will examine Danantara's management and financial responsibility.

This provision aims to assure both domestic and foreign stakeholders who are closely watching the agency's development, particularly regarding potential political intervention in fund utilization. By maintaining a clear audit

framework that reflects transparency, the government hopes to build trust and confidence for potential investors.

### **Challenges of Consolidating with INA**

While both Danantara and INA manage investments, their roles and priorities differ. Danantara is responsible for optimizing state-owned assets and enhancing SOEs performance, whereas INA focuses on attracting global co-investments to fund national infrastructure and development projects. This separation is intended to prevent overlapping mandates and maximize economic impact.

However, a major shift is underway: INA is expected to merge into Danantara as part of a broader consolidation strategy. Inspired by Singapore's investment model, this move seeks to create a unified powerhouse managing Indonesia's strategic investments. Talks are already in progress with key stakeholders to facilitate this transition.

Challenges remain, particularly in aligning the reporting structures of the two entities – INA falls under the Ministry of Finance, while Danantara reports directly to the President. Resolving these structural differences will be critical to achieving an effective integration that strengthens Indonesia's investment strategy.

### **Conclusion**

The establishment of Danantara represents a major shift in Indonesia's approach to SOEs and sovereign wealth management. With plans to consolidate key SOEs and potentially integrate INA, Danantara is intended to streamline asset management, boost investment returns, and attract global capital. However, its success will depend on clear role distinctions, strong governance, and effective implementation. Challenges faced by sovereign wealth funds in other nations highlight the importance of transparency, accountability and strong oversight to ensure stability and investor confidence.

As Danantara takes shape, its impact on Indonesia's economy and investment ecosystem will be closely watched by both domestic and international investors. The coming months should reveal whether this ambitious restructuring can deliver on its promise of a stronger, more efficient sovereign wealth strategy. Stay tuned for the latest updates on Danantara and the Amended SOE Law.

M&T Advisory is a digital publication prepared by the Indonesian law firm, Makarim & Taira S. It informs generally on the topics covered and should not be treated as legal advice or relied upon when making investment or business decisions. Should you have any questions on any matter contained in M&T Advisory, or other comments in general, please contact us at the emails provided at the end of this article.

## CONTACTS



### **Vincent Ariesta Lie**

Partner  
Makarim & Taira S.

**T:** +6221 5080 8300  
**E:** Vincent.lie@  
makarim.com



### **Heru Mardijarto**

Partner  
Makarim & Taira S.

**T:** +6221 5080 8300  
**E:** heru.mardijarto@  
makarim.com



### **Maharanny Hadrianto**

Senior Associate  
Makarim & Taira S.

**T:** +6221 5080 8300  
**E:** maharanny.hadrianto  
@makarim.com



### **Fitria Marsha Qitara Rajasa**

Associate  
Makarim & Taira S.

**T:** +6221 5080 8300  
**E:** fitria.rajasa  
@makarim.com



# MALAYSIA

**SHEARN DELAMORE & CO.**

## Arbitration Legal Update

# How A Confusion Clause Shapes Jurisdiction Battles — Arbitration or Court?

### Introduction

Recently, the English Commercial Court in *Tyson International Company Limited v GIC RE, India, Corporate Member Limited* [2025] EWHC 77 (Comm) (“GIC case”) delivered a significant decision, holding that the English jurisdiction clause prevails over the arbitration clause despite the Court’s generally pro-arbitration stance that Malaysia adopts as well.

### Brief facts of the case

Tyson International Company Ltd (“TICL”) entered into a reinsurance agreement with GIC RE, India, Corporate Member Ltd (“GIC”) through Market Reform Contracts (“MRC”) (policy documents), which contained an English law and jurisdiction clause in the following terms:

*“This Reinsurance shall be governed by and construed according to the Laws of England and Wales. The Courts of England and Wales shall have exclusive jurisdiction of the parties hereto on all matters relating to this insurance.”*

Subsequently, Facultative Certificates (which are based on a US standard form known as Market Uniform Reinsurance Agreement (“MURA”)), were issued in respect of each policy and executed by the parties. The Facultative Certificates contain an arbitration clause and a “Confusion Clause” which states as follows:

*“RI slip [MRC] to take precedence over reinsurance certificate [Facultative Certificates] in case of confusion.”*

A dispute arose over which agreement governed the parties’ obligations. TICL sought an anti-suit injunction in the English courts to prevent GIC from pursuing arbitration in New York, arguing that the MRC should take precedence.

### Court’s decision

The High Court agreed that the facultative certificate was a contractual document, which was intended to supersede the contract found in the MRC (See Court of Appeal’s decision in *Tyson International Company Limited v Partner Reinsurance Europe SE* [2024] EWCA Civ 363 (“Partner Reinsurance case”). In the **Partner Reinsurance case**, a similar jurisdiction challenge was taken where the MRC provided for English Law and jurisdiction clause whilst the subsequent Facultative Certificates contained an arbitration agreement. There, the Court of Appeal stayed the English court proceedings.

However, there was a distinguishing feature in the **GIC case**, as the Facultative Certificates contain a “*Confusion Clause*” which provides that the MRC takes precedence over the Facultative Certificates in case of confusion.

Having found that there was confusion in this case between the jurisdictional clause in the MRC and the arbitration agreement in the Facultative Certificates, the Court held that the English law and jurisdiction clause in MRC prevails.

### **Key takeaways**

The **GIC case** serves as a reminder to drafters of commercial contracts that a “*Confusion Clause*” can influence the Court’s interpretation of jurisdictional provisions in a jurisdictional battle, despite its pro-arbitration stance.

In Malaysia, we find a case similar to the GIC case. In ***Lembaga Pelabuhan Klang v Kuala Dimensi Sdn Bhd*** [2010] 9 CLJ 532, there was an arbitration agreement in the principal agreement and subsequently a supplemental agreement that contained a “submission to court jurisdiction clause”. The Malaysian Court of Appeal refused to stay the Court proceedings pursuant to section 10 of the **Arbitration Act 2005**.

Among others, the Court held that there was an express provision that the supplemental agreement prevails over the principal agreement in the event of any conflict, indicating the parties abandoned the arbitration agreement in the principal agreement by the subsequent supplemental agreement.

*Copyright © 2024 Shearn Delamore & Co. All rights reserved.*

*This Update is issued for the information of the clients of the Firm and covers legal issues in a general way. The contents are not intended to constitute any advice on any specific matter and should not be relied upon as a substitute for detailed legal advice on specific matters or transactions.*

## CONTACT



### **Ching Hao Yan**

Associate, Arbitration &  
Mediation  
Shearn Delamore & Co.

**T:** +603 2027 2925

**E:** chinghaoyan  
@shearndelamore.com



# PHILIPPINES

**MARTINEZ VERGARA & GONZALEZ SOCIEDAD**

## Data Protection Legal Update

# Legal Environment of Data Protection in the Philippines

## Legal Framework

Data protection and cybersecurity are primarily governed by the Data Privacy Act of 2012 (“DPA”) and its implementing rules and regulations (the “DPA Rules”). Cybersecurity is additionally governed by the Cybercrime Prevention Act of 2012 (“CPA”) and its implementing rules and regulations (the “CPA Rules”).

### ***Data Privacy Act of 2012 (Republic Act No. 10173) and Implementing Rules and Regulations***

The DPA and the DPA Rules apply to the processing of all types of personal information and to any natural or juridical person involved in personal information processing including personal information controllers (“PICs”) or personal information processors (“PIPs”), whether in the government or private sector.

The DPA finds extraterritorial application in the following instances:

- a) the PIC or PIP is found or established in the Philippines;
- b) the act, practice, or processing relates to personal information about a Philippine citizen or a resident;
- c) the processing of personal data is being done in the Philippines; and
- d) the PIC or PIP has a link with the Philippines, such as, but not limited to, the following:
  1. use of equipment located in the country, or maintenance of an office, branch or agency in the Philippines for procession of personal data;
  2. a contract is entered in the Philippines;
  3. a juridical entity unincorporated in the Philippines but has central management and control in the country;
  4. an entity that has a branch, agency, office, or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal data;
  5. an entity carries on business in the Philippines; and
  6. an entity that collects or holds personal data in the Philippines.

The DPA and the DPA Rules, however, shall not apply to the following special cases of information, but only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function or activity concerned:

- a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
  - 1. the fact that the individual is or was an officer or employee of the government institution;
  - 2. the title, business address and office telephone number of the individual;
  - 3. the classification, salary range and responsibilities of the position held by the individual; and
  - 4. the name of the individual on a document prepared by the individual in the course of employment with the government.
- b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;
- c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;
- d) Personal information processed for journalistic, artistic, literary or research purposes;
- e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions.
- f) Information necessary for banks and other financial institutions under the jurisdiction of the *Bangko Sentral ng Pilipinas* (the central monetary authority of the Philippines) to comply with the Anti-Money Laundering Act and other applicable laws; and
- g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.<sup>1</sup>

#### ***Key Obligations under the DPA and the DPA Rules***

The DPA and the DPA Rules provide for, among others, guidelines for lawful collection, processing, and retention of personal data, and security measures that PICs are required to undertake.

#### ***Data Privacy Principles***

Processing of personal information must adhere to the principles of transparency, legitimate purpose, and proportionality.

---

<sup>1</sup> Section 6, R.A. No. 10173.

- a) Under the principle of transparency, the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data. Any information and communication relating to the processing of personal data should be easy to access and understand using clear and plain language.
- b) Under the principle of legitimate purpose, personal information may be processed when not prohibited by law and at least one of the following conditions exist, among others:
  - 1. the data subject has given his or her consent;
  - 2. the processing of personal information is necessary and is related to the fulfillment of a contract with the data subject, or in order to take steps at the request of the data subject prior to entering into a contract;
  - 3. the processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
  - 4. the processing is necessary to protect vitally important interests of the data subject, including life and health; or
  - 5. the processing is necessary for the purposes of the legitimate interests pursued by the PIC or by a third party to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.
- c) Under the principle of proportionality, the processing of personal information must be adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose. Personal data must likewise be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

### ***Security Measures***

PICs and PIPs shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data. In determining the level of security appropriate, the nature of the personal data that requires protection, the risks posed by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation are taken into account.

### ***Incident Reporting; Data Breaches***

Data breaches are required to be reported to the National Privacy Commission (“NPC”). Specifically, a notification of personal data breach shall be required under the following circumstances:

- a) when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person; and
- b) the PIC or the NPC believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

In addition to the DPA and the DPA Rules, the NPC issues circulars prescribing policies, rules and regulations, and procedures designed to supplement the DPA and the Rules, and to provide means and measures to carry out their provisions. The NPC likewise issues advisories to serve as guidelines to covered entities and individuals for satisfactory data protection compliance.

The DPA may be accessed through this link: <https://privacy.gov.ph/data-privacy-act/#w3>; and the DPA Rules through this link: <https://privacy.gov.ph/pips-and-pics/advisories-circulars/>. The NPC circulars may be accessed through this link: <https://privacy.gov.ph/pips-and-pics/advisories-circulars/>. NPC advisories may be accessed through this link: <https://privacy.gov.ph/pips-and-pics/advisories-circulars/>

### ***Cybercrime Prevention Act of 2012 (Republic Act No. 10175) and Implementing Rules and Regulations***

The CPA defines acts that constitute cybercrimes. These include:

- a) offences against the confidentiality, integrity, and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices, cybersquatting);
- b) computer-related offences (computer-related forgery, computer-related fraud, computer-related identity theft); and
- c) content-related offences (cybersex, child pornography, cyber libel, unsolicited commercial communications).

The CPA may be accessed through this link: <https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/>; and the CPA Rules through this link: <https://www.officialgazette.gov.ph/2015/08/12/implementing-rules-and-regulations-of-republic-act-no-10175/>.

In addition, all crimes defined and penalized under the Revised Penal Code and other special laws, if committed by, through and with the use of information communications technologies shall be covered by the CPA. These include the following:

- a) ***Electronic Commerce Act of 2002 (Republic Act No. 8792) and Implementing Rules and Regulations***

The Electronic Commerce Act of 2002 (“ECA”) and its implementing rules and regulations (“ECA Rules”) establish the legal recognition of electronic documents and the validity of electronic contracts and signatures, and sets general guidelines for retention and security measures.

The ECA penalizes, among others:

1. hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication

devices, without the knowledge and consent of the owner of the computer or information and communication system; and

2. piracy or the unauthorized copying, reproduction, dissemination, distribution, alteration, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights.

The ECA may be accessed through this link:

<https://www.officialgazette.gov.ph/2000/06/14/republic-act-no-8792-s-2000/>; and the ECA Rules through this link: <https://www.bfar.da.gov.ph/wp-content/uploads/2021/04/Electronic-Commerce-Act-of-2000-R.A.-8792-Implementing-Rules-and-Regulations.pdf>.

- b) *Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act (Republic Act No. 11932)*

The law aims to provide special protections to children from all forms of sexual violence, abuse and exploitation especially those committed with the use of information and communications technology, provides sanctions for their commission, and the implementation of programs for the prevention, deterrence and intervention in all situations of online sexual abuse and exploitation of children in the digital and non-digital production, distribution or possession of child sexual abuse or exploitation material.

The law may be accessed through this link:

[https://lawphil.net/statutes/repacts/ra2022/ra\\_11930\\_2022.html#:~:text=—%20This%20Act%20shall%20be%20known,Materials%20\(CSAEM\)%20Act.%22](https://lawphil.net/statutes/repacts/ra2022/ra_11930_2022.html#:~:text=—%20This%20Act%20shall%20be%20known,Materials%20(CSAEM)%20Act.%22)

- c) *Access Devices Regulation Act of 1998 (Republic Act No. 8484)*

The law regulates the use of access devices or any card, plate, code, account number, electronic serial number, personal identification number, or other telecommunications service, equipment, or instrumental identifier, or other means of account access that can be used to obtain money, good, services, or any other thing of value or to initiate a transfer of funds (other than a transfer originated solely by paper instrument). The law further provides for prohibited acts which constitute access device fraud, including unauthorized possession of access device, and unauthorized disclosure or alteration of information contained in the certain access devices.

The law may be accessed through this link:

<https://acg.pnp.gov.ph/main/quality-policy/17-legal-references/163-ra-8484-access-devices-regulation-act-of-1998.html>.

d) *Anti-Photo and Video Voyeurism Act of 2009 (Republic Act No. 9995)*

The law penalizes the act of taking photo or video coverage of a person or group of persons performing sexual act or any similar activity or of capturing an image of the private area of a person or persons without the latter's consent, under circumstances in which such persons have a reasonable expectation of privacy, or the act of selling, copying, reproducing, broadcasting, sharing, showing or exhibiting the photo or video coverage or recordings of such sexual act or similar activity through without the written consent of the persons involved, notwithstanding that consent to record or take photo or video coverage of same was given by such person.

The law may be accessed through this link:

[https://lawphil.net/statutes/repacts/ra2010/ra\\_9995\\_2010.html](https://lawphil.net/statutes/repacts/ra2010/ra_9995_2010.html).

e) *Subscriber Identity Module (SIM) Registration Act (Republic Act No. 11934)*

This law aims to promote responsibility in the use of SIM and to provide law enforcement agencies the tools to resolve crimes which involve its utilization and to provide a platform to deter the commission of wrongdoings. For this purpose, telecommunications subscribers shall be required to register their SIMs with, and submit personal information to, the public telecommunications entity ("PTE") as a pre-requisite to activation.

The law provides for strict confidentiality of information obtained through registration, subject only to limited instances of authorized disclosure provided for by law, with the corresponding penalties in case of violation.

The law may be accessed through this link:

<https://www.officialgazette.gov.ph/downloads/2022/10oct/20221010-RA-11934-FRM.pdf>

Jurisdiction over cybercrimes shall lie with Philippine courts if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

***The Internet Transactions Act of 2023 (Republic Act No. 11967)***

The Internet Transactions Act of 2023 applies to all business-to-business (B2B) and business-to-consumer (B2C) internet transactions within the mandate of the Department of Trade and Industry (DTI), where one of the parties is situated in the Philippines or where the digital platform, e-retailer, or online merchant is availing of the Philippine market and has minimum contracts. It provides for the rights, regulations, and liabilities of parties in internet transactions, as well as consumer remedies.

The law establishes its own implementing body, the E-Commerce Bureau. Among others, the E-Commerce Bureau is mandated to receive and refer relevant complaints on internet transactions to government agencies such as the NPC.

It likewise provides for the creation of an Online Business Database (OBD) of digital platforms, e-marketplaces, e-retailers, and online merchants engaged in e-

commerce in the Philippines that will provide government and online consumers access to contact information of online businesses. Furthermore, it introduces the “E-Commerce Philippine Trustmark” intended to lend assurance of safety and security in internet transactions.

The DTI is granted ancillary regulatory jurisdiction as to the use of internet for conducting e-commerce by e-marketplaces, online merchants, e-retailers, digital platforms, and third-party platforms under this Act. To this end, it is empowered to issue takedown orders and blacklist online businesses that fail to observe regulatory requirements and compliance orders, which may cover compliance with minimum standards imposed by the NPC.

The Internet Transactions Act of 2023 may be accessed through this link: <https://www.officialgazette.gov.ph/2023/12/05/republic-act-no-11967/>.

#### ***Department of Information and Communications Technology Department Circular No. 002 (2017)***

This circular declares the government policy to adopt a “cloud first” approach and in general adopt cloud computing as the preferred information and communications technology deployment strategy for administrative use and delivery of government online services.

The circular may be accessed through this link: [https://dict.gov.ph/wp-content/uploads/2017/02/Signed\\_DICT-Circular\\_2017-002\\_CloudComp\\_2017Feb07.pdf](https://dict.gov.ph/wp-content/uploads/2017/02/Signed_DICT-Circular_2017-002_CloudComp_2017Feb07.pdf)

#### ***Department of Information and Communications Technology Memorandum Circular No. 005 (2017)***

This circular prescribes the policies, rules and regulations on the protection of Critical Infostructure (CII) as stipulated in the National Cybersecurity Plan (NCSP) 2022. CII refers to the computer systems and/or networks whether physical or virtual, and/or the computer programs, computer data and/or traffic data that vital to the country’s security and national health and safety. Sectors classified as CII include the government, transportation, energy, water, health, emergency services, banking and finance, business process outsourcing, telecommunications and media.

Under this circular, CII are required to, among others: (a) adopt the Code of Practice stipulated in PNS ISO/IEC 27002 and PNS ISO/IEC 27001 on information security management system; (b) participate in the annual risk and vulnerability assessment, and security assessment conducted by the Department of Information and Communications Technology (“DICT”); and (c) secure a Certificate of CyberSecurity Compliance from the DICT.

The circular may be accessed through this link: <https://dict.gov.ph/wp-content/uploads/2017/09/Memorandum-Circular-005.pdf>.

#### **Implementation Mechanism**

The following are the regulatory authorities tasked to implement and enforce the laws relating to data protection and cybersecurity.

***DPA and DPA Rules***

The NPC is tasked with overseeing and enforcing data privacy regulations in the Philippines. The NPC exercises adjudicatory power over complaints and investigations on matters affecting personal data. In the exercise of this function, the NPC may impose cease and desist orders and administrative fines and penalties on natural or juridical persons found violating the provisions of the DPA and the DPA Rules. It may likewise recommend to the DOJ the prosecution of crimes under the DPA. Moreover, it has the authority to impose a temporary ban or a permanent ban on the processing of personal data.

The NPC's official website can be accessed at <https://privacy.gov.ph/>.

***CPA and CPA Rules***

The National Bureau of Investigation ("NBI") and the Philippine National Police ("PNP") are the primary agencies tasked to enforce the CPA and the CPA Rules. Within these agencies, special cybercrime units manned by special investigators are organized to exclusively handle cases involving violations of the CPA and the CPA Rules.

The CPA likewise created under the Department of Justice ("DOJ") the Office of Cybercrime ("DOJ-OCC"), is responsible for coordinating the efforts of the NBI and the PNP in enforcing the provisions of the CPA and the CPA Rules.

The DOJ-Office of Cybercrime (OCC), designated as the central authority in all matters related to cybercrimes, is authorized to, among others:

- a) act as a competent authority for all requests for assistance for investigation or proceedings concerning cybercrimes, facilitate the provisions of legal or technical advice, preservation and production of data, collection of evidence, giving legal information and location of suspects;
- b) act on complaints/referrals, and cause the investigation and prosecution of cybercrimes and other violations of the CPA; and
- c) administer oaths, issue subpoena and summon witnesses to appear in an investigation or proceedings for cybercrime.

Authority to hear and try offenses under the CPA and the CPA Rules and impose penalties for the same lie with the local courts.

DOJ-OCC's website may be accessed at [www.doj.gov.ph/office-of-the-cybercrime.html](http://www.doj.gov.ph/office-of-the-cybercrime.html).

***Judicial Authorities***

The judicial authorities play a crucial role in addressing legal matters related to cybersecurity and personal data protection by ensuring the application of the law and resolving related legal disputes through legal proceedings. Judicial authorities exercise appellate jurisdiction over data privacy matters subject of administrative proceedings before the NPC.

### ***Other Supervisory Authorities***

The **DICT** plays a vital role in cybersecurity governance and policy-making. It works in coordination with other government agencies to strengthen cybersecurity measures.

The DICT supervises cybersecurity through policy development, capacity building, risk assessment, incident response coordination, collaboration with stakeholders, regulatory compliance, and public awareness campaigns. The DICT formulates cybersecurity policies, enhances professionals' skills, assesses risks, coordinates incident response, collaborates with partners, enforces regulations, and educates the public to ensure a secure digital environment.

DICT's official website may be accessed at <https://www.ncert.gov.ph/about-us/dict/>.

The **National Computer Emergency Response Team** ("NCERT"), operating under the DICT, focuses on cybersecurity incident response, threat monitoring, and risk assessment.

The NCERT monitors and responds to cybersecurity incidents, including threats, vulnerabilities, and attacks. The CERT conducts risk assessments, provides early warnings, and coordinates incident response efforts across different sectors. It collaborates with government agencies, organizations, and industry partners to share information, best practices, and expertise.

You can learn more about the NCERT at <https://www.ncert.gov.ph/about-us/dict/>.

### **Data Access**

Except as discussed below, absent any legal requirement, or formal or judicial proceeding, local administrative and judicial authorities may generally not access personal data.

#### ***Under the DPA and DPA Rules***

As discussed, the DPA and the DPA Rules will not apply to information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. We note, however, that the exemption from the requirements of the DPA and the DPA Rules apply only to the minimum extent necessary to achieve the specific purpose, function or activity. The burden of proving that the DPA and the DPA Rules are not applicable falls on those involved in the processing of personal data or the party claiming the non-applicability. In all cases, the determination of any exemption shall be liberally interpreted in favor of the rights and interests of the data subject.

#### ***Under the CPA and CPA Rules***

In the handling of cases involving violations of the CPA and the CPA Rules, the relevant law enforcement authorities are authorized to secure the disclosure or

submission of data by any person or service provider. In relation to such authority, law enforcement is also permitted to perform certain acts in relation to the computer system:

- a) to secure a computer system or a computer data storage medium;
- b) to make and retain a copy of those computer data secured;
- c) to maintain the integrity of the relevant stored computer data;
- d) to conduct forensic analysis or examination of the computer data storage medium; and
- e) to render inaccessible or remove those computer data in the accessed computer or computer and communications network. Law enforcement is also authorized to direct any person with knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information, to enable law enforcement's undertaking of the search, seizure and examination.

The foregoing authorities may, however, only be exercised upon securing a court warrant in relation to a valid complaint officially docketed, and only within the period provided in the search and seizure warrant. Upon the lapse of the period, all computer data examined shall be deposited with the court accompanied by a certification for the law enforcement authorities that no copies have been made or retained. The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or their contents revealed, except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded. Any evidence obtained without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court.

***Under the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act***

The law likewise provides for particular responsibilities of the private sector in relation to handling of content data, traffic data, and subscriber's information relative to the prohibited acts. In particular, internet intermediaries, ISPs, and payment system providers ("PSPs"), such as banks, digital money services businesses, credit card companies and other financial institutions, are required to:

- a) To block, remove, or take down, and report to the DOJ the internet address or websites, or any form of unusual data activity using;
- b) Pursuant to a subpoena issued by the PNP or the NBI, provide the subscriber's or registration information and/or traffic data of any person who:
  1. gained or attempted to gain access to an internet site, internet asset or internet application which contains any form of CSAEM; or
  2. facilitated the violations of the law; or

3. conducted the streaming or live-streaming of child sexual exploitation. The subpoena must particularly describe the information asked for and indicate the relevancy of such information to the sexual abuse and exploitation of children (SAEC) case.

In addition to the above, ISPs shall notify the PNP or the NBI if any form of child sexual abuse or exploitation is being committed using its server or facility, or is likely being committed using its server or facility based on, among others, traffic analysis and observed sudden surges in usage. Internet PSPs having direct knowledge of any OSAEC and CSAEM financial activity shall have the duty to report any suspected OSAEC and CSAEM-related activity or suspicious transaction to the DOJ-OOC and the Anti-Money Laundering Council.

Law enforcement agencies may likewise require financial intermediaries, internet PSPs, and other financial facilitators to provide financial documents and information upon order of any competent court when it has been established that there is reasonable ground to believe that the transactions to be examined involve prohibited activities under the law.

#### ***Under the Subscriber Identity Module (SIM) Registration Act***

PTEs may be required to provide information obtained in the SIM registration process to law enforcement authorities, upon the issuance of a subpoena pursuant to an investigation based on a sworn complaint that a specific mobile number was used as a means to commit a malicious, fraudulent, or unlawful act, and that the complainant is unable to ascertain the identity of the perpetrator.

#### **Cross-border Cooperation**

The Philippines, through the NPC, has been a member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) since 2016. The country is also a member of the Cross-Border Privacy Rules (CBPR) System and is participating in the Global Cross-Border Privacy Rules Declaration together with Canada, Japan, Republic of Korea, Singapore, Chinese Taipei, and the United States of America. The Philippines is also a member of the Global Privacy Assembly (GPA) and is leading the formation of a new working group on “data sharing for the public good” under the GPA.

The Philippines is a member of the Asia-Pacific Economic Cooperation (“APEC”), an intergovernmental forum that promotes economic cooperation among its member economies in the Asia-Pacific region. The APEC has formulated the APEC Privacy Framework which establishes effective privacy protections that are intended to avoid barriers to information flows, ensure continued trade, and economic growth in the Asia-Pacific region. In particular the APEC Privacy Framework intends to establish a common set of privacy principles for member countries in order to improve information sharing as well as provision of technical assistance to other member countries.

The Philippines, along with other ASEAN member states, also partnered with Japan to establish the ASEAN-Japan Cybersecurity Capacity Building Centre. This center aims to enhance cybersecurity capabilities in the ASEAN region through capacity-building programs, knowledge sharing, and technical

cooperation. The collaboration fosters the exchange of best practices and expertise among participating countries.

In February 2018, the Philippines acceded to the Convention in Cybercrime signed on 23 November 2001 in Budapest, Hungary. The Budapest Convention provides for international cooperation for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

In 2024, the Philippines through the NPC, joined the Global Cooperation Arrangement and Privacy Enforcement (Global CAPE), a multilateral arrangement for Privacy Enforcement Authorities to cooperate in cross-border data protection and privacy enforcement.

In addition to its membership in various international organizations, the Philippines has also partnered with different countries to share best practices with regard to personal data protection.

- a) In May 2023, the NPC and Hong Kong's Office of the Privacy Commissioner for Personal Data entered into a Memorandum of Understanding (MoU) on data protection. The collaboration covers provision of mutual assistance in the respective jurisdictions concerning potential contraventions of both countries' privacy and data protection legislation as well as cooperation and joint investigations on cross-border personal data incidents or breaches;
- b) In 2021, the NPC and the United Kingdom's Information Commissioner's Office (ICO) entered into a MoU which formalized their partnership as bilateral partners in sharing best privacy practices;
- c) In 2022, the NPC renewed its MoU with Singapore's Personal Data Protection Commission which aims to share best practices in personal data protection and develop compatible mechanisms to facilitate trusted cross border data flows;
- d) In 2023, the NPC entered into an MoU with the Office of the Privacy Commissioner of Canada (OPCC) with the parties undertaking mutual commitments for assistance in investigations and cooperative efforts in addressing cross-border personal data incidents or breaches;
- e) Still in 2023, the NPC entered into another MoU with the Data Protection Commissioner of the Republic of Malta with a focus on joint research projects and collaboration in the realms of technology and innovation;
- f) In 2024, the NPC entered into a MOU with the Dubai International Finance Centre aimed at strengthening the relationship of the data protection authorities through provision of assistance in enforcement of data protection laws, engaging in joint investigations for data incidents and breaches, knowledge sharing on emerging privacy and data protection trends, and promoting international certification system;
- g) Still in 2024, the NPC and the Personal Information Protection Commission of the Republic of Korea inked a MOU focused on, among others, providing mutual assistance and cooperation for joint investigations while promoting

secure and trusted cross-border data flows, in line with the growth of digital economy;

- h) On 11 February 2025, the NPC and Kişisel Verileri Koruma Kurumu, Türkiye's personal data protection authority, signed a MOU wherein the parties undertook to collaborate by sharing expertise and best practices on data protection policies, education, and training program; and providing mutual assistance in investigating cross-border data breaches and other security incidents;
  - i) Also, on 21 April 2025, the NPC and the Privacy Commissioner of the Islands of Bermuda signed a MOU. The collaboration covers among others, provisions of exchange of information involving potential or on ongoing investigations related to suspected violations of data privacy laws, mutual assistance in facilitating such investigations in their respective jurisdictions, coordination and provision of support in joint investigations involving cross-border personal data incidents or breaches, assistance in enforcing decisions and resolutions issued by either party concerning data protection within their own jurisdictions; and
  - j) Finally, just this 24 April 2025, the NPC and the Israeli Privacy Protection Authority signed a MOU establishing a framework for promoting collaboration and cooperation between the Philippines and Israel in personal data protection and cross-border enforcement.
-

## CONTACTS



**Erika B. Paulino**

Head, Data Privacy and Security  
Martinez Vergara & Gonzalez Sociedad

**T:** +63 2 8687 1195

**E:** Erika.paulino@mvgslaw.com



**Kristine R. Bongaron**

Co-Head, Data Privacy and Security  
Martinez Vergara & Gonzalez Sociedad

**T:** +63 2 8687 1195

**E:** Kristine.bongaron@mvgslaw.com



# CAMBODIA

**TILLEKE & GIBBINS**

## Employment Legal Update

# Funding Cuts and Mass Layoffs Due to Financial Stress in Cambodia

The recent freeze on US foreign aid has led to the suspension of billions of dollars in foreign assistance as well as widespread layoffs at contracting organizations around the world. Under this situation, USAID-funded offices in all jurisdictions, including Cambodia, may face the challenge of determining whether they need to lay off their employees.

Employers in Cambodia may take different steps in response to this and other instances of sudden financial stress in order to manage their workforce in accordance with Cambodian laws and regulations.

### Suspension

Cambodia's Labor Law allows employers to suspend employment contracts due to a major economic or material issue or any unexpected difficulty that results in the suspension of operations. To impose this employment contract suspension, the employer must initially submit a suspension request to the Ministry of Labor and Vocational Training (MLVT), detailing the reasons for the requested suspension.

If the reasons are deemed valid and the request is approved, the suspension period cannot exceed two months. During the suspension period, the employer must continue providing accommodation for employees if this benefit is already being provided. In some circumstances, the suspension period can be extended if necessary (as happened during the COVID-19 pandemic).

However, financial difficulties alone may not be a valid reason for extension. The decision is at the discretion of the MLVT labor inspectors on a case-by-case basis. Therefore, given the uncertain timeline of financial difficulties that may significantly impact the employer's budget, suspending employment contracts might be ineffective.

### Mass Layoffs

Under Cambodia's Labor Law, mass layoffs due to a significant reduction in an establishment's operation or an internal reorganization foreseen by the employer are permissible.

The layoff order must be based on professional qualifications, seniority period, and family burdens of the employees. The first employees to be laid off must be those with the least professional ability, followed by those with the least seniority. For seniority calculations, married employees must be given an additional year, as well as an additional year for each dependent child.

In addition, employers must inform the employees' representatives in writing to solicit their suggestions, primarily on measures for announcing employee reductions in advance and minimizing the effects on affected workers.

The mass layoffs procedure is subject to the MLVT's review and approval. Upon receipt of the request, an MLVT labor inspector may conduct a hearing to examine the impact of the proposed layoffs and measures to be taken to minimize their effects.

### **Termination**

If an employment contract is not terminated by mutual agreement, due to serious misconduct by either party, or force majeure as defined under the Labor Law, the termination must have a valid reason.

Under the Labor Law, "valid reason" may refer to an employee's aptitude or behavior, based on the requirements of the operation of the establishment. However, if employers face financial difficulties, they may consider declaring bankruptcy.

Declaring bankruptcy can be considered a valid reason and exempts employers from paying damages, as it does not impact an employee's dignity or cause the public to question their behavior, abilities, or performance. However, declaring bankruptcy has legal implications, as it is governed by the Law on Insolvency and requires court proceedings.

The process involves filing an insolvency complaint with the court, which will review the complaint to determine if the employer is indeed insolvent. In addition, the employer must notify employees about the insolvency proceedings, their rights, and any potential layoffs. Employees can file claims for unpaid wages and other compensation, which are prioritized over other unsecured debts under both the Law on Insolvency and the Labor Law. Employers' assets can be sold to pay off creditors, with employees being among the first to receive payment.

### **Damages and Statutory Payments**

According to the Notification on Compensation for Terminating an Employment Contract, dated March 21, 2024, employers that terminate an employment contract without a valid reason must pay damages to the employees as follows:

- a) For employees under a fixed-duration contract, the damages must be at least equal to the wages the employee would have received if they had completed the original term of the contract; and
- b) For employees under an unspecified-duration contract, the damages are equal to the seniority payment received during the employment contract.

These damages are in addition to required statutory payments that employees must receive after their contract is terminated, detailed in the table below.

Type of Employment Contract	Statutory Payments
Fixed duration	<ul style="list-style-type: none"> <li>• Wages that have not yet been paid;</li> <li>• Unused and unpaid annual leave through the termination date; and</li> <li>• Severance payment equal to at least 5% of the wages paid to the employee during the length of the contract.</li> </ul>
Unspecified duration	<ul style="list-style-type: none"> <li>• Wages that have not yet been paid;</li> <li>• Unused and unpaid annual leave through the termination date;</li> <li>• Compensation in lieu of a notice if the employer did not give prior notice in accordance with the Labor Law; and</li> <li>• Seniority indemnity for the semester that the employee is terminated and total seniority back payments that have not been paid.</li> </ul>

The requirements regarding statutory payments and other compensation dues to employees upon termination of employment were significantly [clarified by a notification in March 2024](#).

**Compliance**

Organizations forced to consider mass layoffs should consult with legal counsel to ensure compliance with the March 2024 notification and other relevant labor regulations before proceeding with any workforce reduction measures. Proactive communication with both the MLVT and employee representatives will be crucial throughout this process. Furthermore, employers should consider developing contingency plans that account for various timelines of financial recovery, as each approach—whether suspension, mass layoffs, or termination—carries distinct legal obligations and financial implications that extend beyond the immediate crisis period. Organizations that approach these difficult decisions with careful planning and legal diligence will be better positioned to maintain operational stability while fulfilling their obligations to employees during this period of economic uncertainty.

## CONTACTS



### Jay Cohen

Partner and Director,  
Cambodia practice  
Tilleke & Gibbins

**T:** +855 23 964 210  
**E:** [jay.c@tilleke.com](mailto:jay.c@tilleke.com)



### Mealtey Oeurn

Associate,  
Corporate and Commercial  
Tilleke & Gibbins

**T:** +855 23 964 210  
**E:** [mealtey.o@tilleke.com](mailto:mealtey.o@tilleke.com)



# LAOS

**TILLEKE & GIBBINS**

## Banking & Finance Legal Update

### New Regulations on Foreign Currency in Laos

On January 3, 2025, the Bank of the Lao PDR (BOL) issued Decision No. 11/BOL on the Use of Foreign Currency in Lao PDR, taking effect on the same date. This decision sets out the rules for using foreign currency in Laos and ensures the Lao kip (LAK) remains the primary currency while allowing flexibility for international transactions.

Key points in the decision are outlined below.

#### **Permissible Activities for Foreign Currency**

The decision provides that authorized entities can use foreign currency as a secondary currency to LAK in the setting of cost and pricing structures, announcing and advertising prices, and making or receiving payments for goods and services that are imported or have manufacturing inputs imported from other countries. Otherwise, LAK is the only permitted currency.

The decision also stipulates that foreign exchange must be conducted only via authorized commercial banks or foreign exchange markets. The exchange rate for setting costs, pricing structures, announcing and advertising prices, and making and receiving payments for goods and services in foreign currency must match the exchange rate announced by commercial banks from time to time.

#### **Businesses Allowed to Use Foreign Currency**

The decision allows certain businesses and organizations to use foreign currency. These entities are divided into two groups: those that need approval before using foreign currency, and those that can use it immediately.

Enterprises that can use foreign currency with BOL approval include:

- a) Businesses that export goods or services and entities that lease or obtain concessions from the government, generating revenue in foreign currency through commercial banks;
- b) Enterprises that provide international freight and passenger transportation services;
- c) Enterprises that provide services related to cross-border logistics and warehousing;
- d) Enterprises located at international borders and airports, such as duty-free shops and restaurants;
- e) Enterprises that have obligations to make payments in foreign currency to other countries and suppliers of goods and services to exporters that generate income in foreign currency from exporting;
- f) Enterprises operating international insurance, such as travel insure, overseas project insurance, transport insurance, and reinsurance;

- g) Tour agencies;
- h) Enterprises operating casino businesses that receive service fees within the scope of their business activities; and
- i) Other businesses that may be allowed to use foreign currency after obtaining approval from the BOL.

Entities in the government sector, enterprises providing accommodation services, embassies, consulates, and commercial banks and use foreign currency immediately under certain circumstances:

- a) Government sector entities
  - 1. Making or receiving donations via commercial banks; and
  - 2. Collecting state budget revenue at borders and international airports, including service and visa fees and obligatory state fees related to arrivals and departures in Laos.
- b) Embassies and foreign consulates
  - 1. Receiving payments, setting values, and announcing visa and service fees related to travel to their countries; and
  - 2. Making or receiving payments, setting values, and announcing or advertising fees, service charges, interest, and other fees related to their transactions through commercial banks.
- c) Enterprises operating accommodation services
  - 1. Announcing and advertising service fees through online media using foreign languages; and
  - 2. Accepting payments from other countries via electronic payment tools, with payments made to their bank accounts opened with commercial banks in the Lao PDR.

### **Requesting Approval to Use Foreign Currency**

Entities that are required to obtain approval from the BOL prior to using foreign currency in Laos must submit a request letter stating the reasons, along with supporting documents. These documents include relevant certificates and licenses, a revenue-expense plan in LAK and foreign currency, and a foreign currency exchange plan for a period of one year.

A determination will be made within ten working days of receiving accurate and complete documents and will be valid for a period of one year from the issuance date.

**Penalties**

The decision prohibits entities from using foreign currency outside the approved scope, setting and announcing foreign exchange rates without obtaining approval from the BOL, making payments in foreign currency via unauthorized systems, rejecting or avoiding selling foreign currency to commercial banks based in Laos, and other behaviors that violate the law. Violators will be reeducated or fined, with fines doubling for repeat offenses. Persistent violations may lead to the revocation of the approval certificate for using foreign currency in Laos or rejection of certificate renewal, with an announcement to the public.

---

**CONTACTS**



**Prisna Sungwana**

Partner and Director,  
Banking & Finance  
Tilleke & Gibbins

**T:** +66 2056 5656  
**E:** prisna.s@tilleke.com



**Sayphin Singsouvong**

Associate, Banking &  
Finance  
Tilleke & Gibbins

**T:** +856 21 262 355  
**E:** sayphin.s@tilleke.com



**Naiyane Xaechao**

Associate, Corporate and  
Commercial  
Tilleke & Gibbins

**T:** +856 21 262 355  
**E:** naiyane.x@tilleke.com

## Life Sciences Legal Update

# Laos' New Regulation on Biopharmaceuticals, Gene Therapy, and Stem Cells

On November 22, 2024, the Ministry of Health (MOH) in Laos issued Decision No. 3730/MOH, which regulates the management, processing, production, and use of biopharmaceutical products, genes, and stem cells. This decision came into force on January 18, 2025, 45 days after its publication in the *Lao Official Gazette* on December 4, 2024. This decision signifies Laos' recognition and acceptance of biopharmaceutical products, genes, and stem cells for use in medical treatments and the beauty industry, and it aligns with the ongoing development of biomedical sciences in the country.

### Definitions

The MOH's decision defines biopharmaceuticals, gene therapy, and stem cells as follows:

- a) "Biopharmaceutical products" refers to a type of biological or drug product that is produced or synthesized from natural substances, objects, or chemicals. This group of products includes blood, blood components, allergens, cells or cellular components, gene therapies, tissues, protein-based medicines, drugs derived from living cells, and biologics, which can be produced from sugars, proteins, amino acids, or substances with complex characteristics derived from organic sources such as human, animal, and plant parts; yeast; and microorganisms. These products exclude vaccines and biosimilar products, which will be specified under separate regulations.
- b) "Gene therapy" refers to a treatment approach that applies the principle of arranging amino acids (which could involve DNA or RNA sent to the patient's cells in the form of a drug with the purpose of treating a certain disease).
- c) "Stem cells" are defined in the decision as cells or immature cells that can be sourced from various organs in the body. They are characterized by being undifferentiated, having the potential for differentiation, and being self-renewing.

### Stem Cell Production

The decision outlines comprehensive provisions for managing and using raw materials in stem cell production. Key points include:

- a) **Production location standards:** Ensuring facilities meet specific standards of the MOH.
- b) **Personnel nationality restrictions:** Limiting certain roles to Lao nationals—for instance, product managers, quality control managers, and quality assurance managers.

- c) **Raw material requirements:** Complying with ethics committee guidelines, including prohibitions on using embryos and fetuses.
- d) **Product consent agreement:** Before using certain types of stem cell products on a patient, consent must be obtained from a fully conscious patient and witnessed by a relative. If a patient is unconscious, consent for treatment or services must be obtained from a relative in accordance with ethical guidelines.
- e) **Compensation for damages resulting from use:** The consent form for treatment must specify the conditions for compensation for damages resulting from the use of the product in accordance with the treatment conditions set out in the consent form.

### **Importation and Exportation**

For importing biopharmaceutical products, genetic material, and stem cells, applicants must submit complete documentation, including an enterprise registration certificate, production license, and product quality certificate. Strict quality inspections and compliance with the Law on Drugs and Medical Products are mandatory. Additionally, the importation of raw materials from embryos and fetuses is prohibited.

Exporters must also provide comprehensive documentation, including an exportation approval certificate, product registration certificate, and quality inspection report. They must ensure product quality through rigorous inspections and comply with both local and destination country regulations.

### **Clinical Trial Management**

This decision defines a clinical trial as “a scientific process that designs and conducts experiments on the human body. The interpretation of the research results aims to provide an understanding of the principles and guidelines for the use of drugs, devices, instruments, and procedures in treating patients.” Clinical trials must be authorized by the MOH’s Food and Drug Department (FDD) through the approval of an ethics committee. All procedures, processes, and actions related to the clinical trial must be approved by the FDD, which will approve the conduct of a clinical trial if it is assessed to be beneficial for the development of disease prevention and treatment in Laos.

### **Business Operating Requirements**

To operate a business involving stem cells, operators must:

- a) Obtain licenses from relevant sectors, including planning and investment, natural resources and environment, and health;
- b) Be Lao nationals with relevant qualifications;
- c) Undergo regular inspections and evaluations by the MOH; and
- d) Employ specialists with appropriate qualifications and experience.

Businesses operating in the biopharmaceutical, gene therapy, and stem cell sectors in Laos must navigate a complex regulatory landscape under Decision No. 3730/MOH. The decision establishes clear compliance requirements, from facility standards and personnel restrictions to ethical sourcing and quality control. Companies seeking to enter or expand in this market should closely monitor further regulatory developments and ensure strict adherence to MOH guidelines. As Laos continues to develop its biomedical sector, businesses that align with these regulations and invest in compliance infrastructure will be well-positioned for long-term growth and market stability.

---

## CONTACTS



**Prisna Sungwanna**

Partner and Director,  
Banking & Finance  
Tilleke & Gibbins

**T:** +66 2056 5656  
**E:** prisna.s@tilleke.com



**Naiyane Xaechao**

Associate, Corporate and  
Commercial  
Tilleke & Gibbins

**T:** +856 21 262 355  
**E:** naiyane.x@tilleke.com



# MYANMAR

TILLEKE & GIBBINS

## Corporate/M&A Legal Update

# Myanmar Changes Documentation Rules for Share Transfers and Director Appointments

Myanmar's Directorate of Investment and Company Administration (DICA) has issued new documentation requirements for Myanmar-registered companies making changes to their shares or directors. Effective January 8, 2025, the DICA will only approve such changes when accompanied by specific supporting evidence as required under the Myanmar Companies Law 2017 (MCL).

### **Key Changes and Requirements**

For share transfers, companies must submit the required application form, along with the following documents:

- a) Resolution from the company's board of directors approving the change of shares or share transfer; and
- b) Copy of the share-transfer agreement signed by both parties, with proof of stamp duty payment.

For director changes, companies must submit the required application form, along with the following documents:

- a) Copy of new director's ID or passport;
- b) Shareholder resolution approving the change of the director(s); and
- c) New director's consent to act (for appointments) or signed resignation (for departures)

In addition to announcing the new documentation requirements, the DICA also reminded companies of an April 2023 announcement that requires companies to submit certain other [required documentation within two months of establishment](#) to the DICA by email.

### **Next Steps**

Companies planning share transfers or director changes must ensure they prepare the complete documentation package before submission to the DICA.

For more information on this announcement or assistance with corporate secretarial matters, please contact Tilleke & Gibbins at [myanmar@tilleke.com](mailto:myanmar@tilleke.com).

## CONTACTS



### **Yuwadee Theanngarm**

Partner and Director,  
Corporate and  
Commercial  
Tilleke & Gibbins

**T:** +95 9 772 440 002  
**E:** yuwadee.t  
@tilleke.com



### **Aye Thuzar Hlaing**

Senior Associate,  
Corporate and  
Commercial  
Tilleke & Gibbins

**T:** +95 9 772 440 001  
**E:** AyeThuzarHlaing  
@tilleke.com



### **Khin Pearl Yuki Aung**

Consultant, Corporate  
and Commercial  
Tilleke & Gibbins

**T:** +95 9 772 440 001  
**E:** yukiaung  
@tilleke.com

## Technology Legal Update

### Myanmar Issues Cybersecurity Law

On January 1, 2025, Myanmar's State Administration Council enacted Cybersecurity Law No. 1/2025, which aims to regulate various aspects of digital security and online activities. The law has not yet been implemented and will come into force on a date specified by the Myanmar president, who will also provide an official adoption and compliance timeline for individuals and organizations impacted by the new regulations.

Below are some of the key provisions, implications, and penalties under the Cybersecurity Law.

- a) **Extraterritorial penalties.** The law contains an important provision that authorizes penalties against Myanmar citizens who are found guilty of violations, even if these occur outside the country's borders.
- b) **VPN definition and regulation.** Virtual private networks (VPNs) are defined by this law as specific systems that function as backup networks by using technological means in order to ensure the safety of linking networks to each other. This definition sets the framework for subsequent regulations and penalties associated with VPN usage. The law does not restrict individuals or entities from using VPNs; it regulates VPN service providers.
- c) **Penalties for unapproved VPN services.** Establishing a VPN or providing VPN services without approval from the designated ministry (to be appointed later by the government) can result in significant penalties. For individuals, the punishment may be imprisonment for 1–6 months, a fine of MMK 1–10 million (approx. USD 476–4,760), or both, with the proceeds of the violation being confiscated. If the violator is a company or organization, the minimum fine will be MMK 10 million, and the proceeds will be confiscated.
- d) **Government oversight.** The ministry designated by the government is authorized to investigate and take control of cybersecurity services and digital platform services for national defense and security purposes, or upon request from a government department or organization in accordance with respective laws.
- e) **Licensing requirements.** The Cybersecurity Law introduces two types of licenses, valid for a period of 3–10 years, for (1) cybersecurity services and (2) digital platform providers. Digital platforms with over 100,000 users are required to apply for the latter license. Noncompliance with this requirement will be subject to a fine of at least MMK 100 million (approx. USD 47,600), and any proceeds resulting from the violation will be confiscated.
- f) **Penalties for unsolicited communications.** Individuals who transmit unwanted and unsolicited messages, emails, or data via a network will be subject to imprisonment for 1–2 years, a fine of MMK 5–20 million (approx. USD 2,380–9,530), or both.

- g) **Penalties for cyber misuse.** Engaging in cyber misuse—including the alteration, deletion, or sale of computer programs or data, as well as the unauthorized control and execution of computer systems, programs, or electronic data—will be subject to imprisonment from 6 months to 3 years, a fine of MMK 1–20 million (approx. USD 476–9,530), or both.
- h) **Penalties for online theft or mischief.** Committing or inciting others to commit online theft or mischief using cyber resources will be subject to imprisonment for 2–7 years and the possibility of additional fines.
- i) **Penalties for unapproved online gambling.** Operating an online gambling system without proper authorization may result in imprisonment for 6 months to 1 year, a fine of MMK 5–20 million (approx. USD 2,380–9,530), or both, with the proceeds from such activities being confiscated. If the offender is a corporation or organization, the minimum fine is MMK 20 million, and the illicit proceeds will also be confiscated. The law does not address how online gambling platforms can obtain official approval.

Myanmar's Cybersecurity Law represents a significant step in the country's regulation and oversight of digital security and online activities. Businesses, digital platform providers, cybersecurity service providers, and VPN providers need to understand these requirements and ensure compliance to prevent substantial penalties.

For more details on the Cybersecurity Law, or on any aspect of digital security and internet regulations in Myanmar, please contact Tilleke & Gibbins at [myanmar@tilleke.com](mailto:myanmar@tilleke.com).

---

## CONTACTS



### **Yuwadee Thean-ngarm**

Partner and Director,  
Corporate and  
Commercial  
Tilleke & Gibbins

**T:** +95 9 772 440 002  
**E:** yuwadee.t@tilleke.com



### **Nwe Oo**

Senior Associate,  
Corporate and  
Commercial  
Tilleke & Gibbins

**T:** +95 9 772 440 001  
**E:** nweoo@tilleke.com



### **Aye Thuzar Hlaing**

Senior Associate,  
Corporate and  
Commercial  
Tilleke & Gibbins

**T:** +95 9 772 440 001  
**E:** AyeThuzarHlaing@tilleke.com



# THAILAND

**TILLEKE & GIBBINS**

## Technology Legal Update

### Thailand Amends Emergency Decree on Technology Crime

On April 12, 2025, Thailand published an amendment to the Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes in the *Government Gazette*, with the regulation taking effect the following day.

Drafts of the amendment had been [shared in recent months](#), and the final amendment of the decree contains some additional key revisions, such as narrowing the business operators subject to the decree's requirements, reducing operators' obligations, and establishing collaboration between relevant stakeholders to tackle technology crime.

These key revisions to the amendment are detailed below.

- a) **Business operators subject to the decree:** The business operators covered under the decree now include only payment service providers under the Payment System Act and digital asset operators under the Royal Decree on Digital Asset Businesses. Digital platform services under the Royal Decree on Digital Platform Service Businesses That Are Subject to Prior Notification are no longer within the scope of the decree.
- b) **Definition of technology crime:** The final version of the amendment removed the expanded definition of technology crime that had been included in a previous draft, leaving the decree's existing definition unchanged.
- c) **Telecommunications provider obligations:** Mobile and telecommunications service providers now have an obligation to monitor and screen for content that may be related to technology crime and suspend SIM cards when instructed to do so by the National Broadcasting and Telecommunications Commission (NBTC).
- d) **Transaction and account suspension:** The amendment removes the decree's complex transaction suspension procedures and leaves room for business-specific regulators (e.g., Bank of Thailand, Securities and Exchange Commission, NBTC) to impose various technology crime suspension requirements on business operators under their supervision. The newly established Center for Prevention and Suppression of Technology Crimes can also notify financial institutions and business operators of names or digital asset wallet addresses that may be related to technology crime, triggering an obligation to suspend the accounts.
- e) **Shared liability:** Although digital platform service providers are not in the scope of business operators under the amended decree, online social media platform operators are still jointly accountable with other operators (i.e., financial institutions, business operators, and related service providers) for damages from technology crime. To be released from this liability, operators have to prove their compliance with the technology crime standards and measures stipulated by their regulators (safe harbor rules).

Business operators will need to wait and see how their sector-specific regulators impose requirements to combat technology crime. Online social media platforms

should closely monitor the safe harbor rules, which are expected to be issued soon.

For more details on any aspect of technology and cybersecurity in Thailand, please contact any of the lawyers listed below.

---

## CONTACTS



**Athistha (Nop)  
Chitranukroh**

Partner and Director,  
Corporate and  
Commercial  
Tilleke & Gibbins

**T:** +66 2056 5600  
**E:** [nop.c@tilleke.com](mailto:nop.c@tilleke.com)



**Pornpan Wichawut**

Counsel  
Tilleke & Gibbins

**T:** +66 2056 5707  
**E:** [pornpan.w@tillike.com](mailto:pornpan.w@tillike.com)



**Thammapas  
Chanpanich**

Associate, Corporate  
and Commercial  
Tilleke & Gibbins

**T:** +66 2056 5561  
**E:** [thammapas.c@tilleke.com](mailto:thammapas.c@tilleke.com)

## CONTACTS



**Rujaporn  
Paritsantik**

Associate, Corporate  
and Commercial  
Tilleke & Gibbins

**T:** +66 2056 5539

**E:** rujaporn.p  
@tillike.com



**Rada Lamsam**

Associate, Corporate  
and Commercial  
Tilleke & Gibbins

**T:** +66 2056 5713

**E:** rada.l@tillike.com

## Intellectual Property Legal Update

### The Intellectual Property Implications of Thailand's Entertainment Complex Bill

Thailand's aim of hosting entertainment complexes that include casinos is moving forward with the cabinet's approval in principle of the draft Entertainment Complex Business Act on January 13, 2025.

In fact, Thailand has studied the pros and cons of allowing the operation of entertainment complexes since March 2019. Though the initial surge of global interest died down during the COVID-19 pandemic, the country renewed its efforts with the recent draft law. This is part of the government's aim of bringing parts of the informal economy (or shadow economy) and the underground economy—estimated to be more than 50% of Thailand's GDP—into the revenue system.

While many authors have provided analyses of the bill's contents, this article explores how the enforcement of the Entertainment Complex Bill after its passage would relate to various aspects of intellectual property (IP) in the casino business in the context of Thai law. Below are some examples of the potential effects of the draft legislation on IP rights in Thailand.

#### **Public Order and Public Policy**

Under Thai law, contradiction of public order, good morality, or public policy is grounds for denying IP protection. With the eventual passage and enforcement of the Entertainment Complex Bill, IP rights related to gaming that used to be regarded as contrary to the public order and received no protection under the current law would become eligible for legal protection and considered registrable under the law. This is similar to what happened recently with cannabis in Thailand. Legalization of cannabis opened up pathways for trademark and patent protection in this industry.

IP in the casino industry encompasses a wide range of assets, including patents, trademarks, copyrights, and trade secrets. These IP rights protect the unique features of casino games, gaming machines, software, and branding elements. For instance, in Thailand patents can cover technical solutions when connected to innovative hardware, while trademarks protect the names and logos of casinos, resorts, games, and retail offerings in these locations. If the change in Thai law makes possible the registration of this IP, it would benefit not only the entertainment complex or casino operator but also inventors, artists, and the general public by allowing them to receive IP protection for their creations or inventions related to casinos and gambling.

#### **IP Licensing and Technology Transfer**

The casino industry is a dynamic and rapidly evolving sector that relies heavily on IP to protect its innovations and maintain a competitive edge. As casinos expand their digital presence and introduce new gaming technologies, finance and accounting solutions, and loyalty programs, the importance of IP licensing becomes increasingly significant. IP licensing allows casino and integrated resort

operators to use and commercialize third-party IP. This is particularly crucial in the casino industry, where the process of adopting new games and technologies often involves collaboration with third-party developers and manufacturers. Licensing agreements ensure that all parties involved can benefit from the use of IP while protecting the rights of the original creators.

Legalization of the gaming industry will foster technology transfer to Thailand, which could involve various IP rights. For example:

- a) **Patent licensing:** Patents protect the technical aspects of gaming machines. For example, a patent for a new slot machine mechanism can be licensed to multiple casinos, generating revenue for the patent holder through royalties;
- b) **Trademark licensing:** Licensing trademarks enables casinos to use well-known brands and logos, attracting customers and building trust. For instance, a local casino developer may license the trademark of a well-known casino brand or license a popular game to offer it exclusively at their venue;
- c) **Copyright licensing:** Copyrights protect the software, artistic works, and musical elements of casino games. Licensing copyright allows casinos to legally use copyright content, such as game graphics, user interfaces, and soundtracks; and
- d) **Trade secret/know-how licensing:** Unregistered IP, such as trade secrets and know-how in the gaming industry, could include proprietary operations systems, ongoing technical services, and consultancy services provided by experienced operators.

Other areas of IP protection include design protection for the unique design of the machine or equipment and trade dress protection for the distinctive elements of gaming machines or casino decorations.

Thailand's Entertainment Complex Bill stipulates that the gaming machines used in casinos must be up to the standard set by the Entertainment Complex Policy Board, in good shape, and able to operate without errors. The operator must also assist government officials in inspecting and testing the gaming machines in the casino. Any operator who fails to resolve an issue within the given time could face a penalty of up to THB 500,000 (approx. USD 14,380) per day until the issue is resolved.

Noting the necessity of complying with these potentially complex standards for gaming machines, it is therefore important to use machines with proven reliability. As the associated intellectual property rights have not been registrable in Thailand (as discussed above), technology transfer will be required for entertainment complex operators in Thailand, and the focal point for this technology transfer will be patents, copyright (computer programs), and trade secrets.

### **IP Clearance**

Operators will also need to ensure they are not infringing on others' IP rights. It is thus necessary to conduct IP clearance or freedom-to-operate searches before

launching operations or using any content or technology, especially when it is not owned or invented by the entertainment complex operator. Conducting an IP clearance search can prevent costly legal disputes and the potential need to rebrand or cease operations after the launch of the business. This proactive step saves time and resources and guards against the reputational damage that could arise from an infringement suit.

### **Data protection and compliance**

The collection, use, and protection of players' personal data is a growing concern within the gaming and integrated resort industries. Thailand's Personal Data Protection Act of 2019 (PDPA) sets out a regulatory framework for this. Investigations into and enforcement of the PDPA are progressing in Thailand. Recently, a major company was fined THB 7 million for its noncompliance, highlighting the importance of adhering to PDPA requirements. Additionally, the regulator has introduced a new "compliance checklist" with ten key areas of focus, indicating a shift toward more stringent regulatory requirements and oversight.

The Entertainment Complex Bill would also regulate other aspects related to casinos, like advertising and promotion, casino licensing requirements, minimum investment requirements, taxation, allowed types of gaming machines, operating times, time and place restrictions on selling alcoholic beverages, and casino entry requirements. We have discussed some of these requirements in [another article](#).

### **Outlook**

The Entertainment Complex Bill is preparing to open up various types of business opportunities to investment from both domestic and international actors, whether directly as an entertainment complex operator or as a licensor of IP or transferor for technology. Emerging technologies, such as virtual reality and blockchain, are set to revolutionize the gaming experience, creating new opportunities for IP licensing.

Gaming operators and integrated resorts that effectively manage their IP assets and establish strong licensing agreements will be well-positioned to thrive in this competitive market. For companies considering an entry into the prospective Thai market for entertainment complexes, preparing now for future IP filings will provide a strong foundation that will facilitate efficient operations, assuming the Entertainment Complex Bill is passed in a form similar to the existing draft.

## CONTACTS



**Nuttaphol  
Arammuang**

Partner, Intellectual  
Property  
Tilleke & Gibbins

**T:** +66 2056 5896

**E:** [nuttaphol.a@tilleke.com](mailto:nuttaphol.a@tilleke.com)



**Alan Adcock**

Partner and Director,  
Intellectual Property  
Tilleke & Gibbins

**T:** +66 2056 5871

**E:** [alan.a@tilleke.com](mailto:alan.a@tilleke.com)

A faint, light-colored map of Southeast Asia is visible in the background, showing the outlines of Vietnam, Laos, Cambodia, Thailand, Malaysia, and Indonesia. The map is centered and serves as a subtle backdrop for the text.

# VIETNAM

**TILLEKE & GIBBINS**

## Regulatory Affairs Legal Update

### Vietnam's Government Restructuring: Key Changes and Implications for Businesses

Vietnam's political system is currently undergoing a significant reorganization to streamline government operations and improve efficiency. In this regard, Plan 141/KH-BCDTKNQ18, issued on December 6, 2024, provided guidelines on the restructuring of existing ministries, ministerial-level agencies, and government-affiliated agencies. Accordingly, the number of ministries is being reduced from 18 to 14 through mergers and consolidations and the establishment of a new Ministry of Ethnic and Religious Affairs. The number of ministerial-level agencies is being reduced to three, and government-affiliated agencies to five. Similar streamlining is happening at provincial levels.

The newly consolidated state agencies will assume all functions, rights, and responsibilities of the merged entities, and will continue handling all ongoing matters previously handled by the former agencies. Some examples of these changes include the following:

- a) The Ministry of Science and Technology (MOST) will oversee telecommunications, IT applications, cybersecurity, e-transactions, and national digital transformation, which had previously been managed by the Ministry of Information and Communications (MIC). MOST will also be responsible for issuing licenses related to these areas, such as licenses for G1 online game services and telecommunication services. The Ministry of Culture, Sports, and Tourism will assume the responsibility of press management, previously under the MIC.
- b) The Ministry of Finance will assume state management functions related to investment, previously handled by the Ministry of Planning and Investment. Provincial Departments of Finance will issue Investment Registration Certificates and Enterprise Registration Certificates, a responsibility previously held by the Departments of Planning and Investment.
- c) The Ministry of Home Affairs will oversee labor and employment matters. Provincial Departments of Home Affairs will be authorized to issue work permits and will be the designated authorities for companies to register their internal labor regulations.

#### **Advantages for Businesses**

The restructuring aims to simplify regulations and expedite licensing processes. By reducing the number of agencies and streamlining their functions, businesses can expect to encounter fewer bureaucratic hurdles and experience faster processing times for permits, licenses, and approvals.

In addition, the government's focus on attracting and retaining top talent through measures like increased salaries, allowances, and benefits (as outlined in Decree No. 179/2024/ND-CP) is expected to result in a more professional and efficient public sector. This, in turn, will lead to more informed and timely decision-making. With a more streamlined government structure, businesses can potentially save time and resources by dealing with fewer government agencies. This can

significantly reduce the administrative burden on businesses and free up resources for core activities such as product development, service innovation, and customer acquisition.

### **Potential Challenges**

The government restructuring, while aiming for long-term benefits, may present some temporary challenges for businesses, including:

- a) **Disruptions during reorganization:** As the newly formed agencies undergo internal restructuring, they may experience delays in resuming their normal operations. This can lead to temporary slowdowns in processing applications, issuing licenses, and handling other business-related interactions.
- b) **Uncertainty due to regulatory changes:** The restructuring will likely involve changes in regulations and procedures governing various industries. This transitional period may create uncertainty for businesses as they navigate the evolving regulatory landscape. New state agencies might face delays in fully taking on their duties, which could lead to hesitancy in issuing licenses or making important decisions while they get used to their new roles. Additionally, changes in regulatory procedures might happen before the laws are updated, creating gaps in the legal framework and potentially slowing down decision-making by authorities.
- c) **Potential need for new licenses and permits:** While existing licenses or permits issued under the former agency structure may remain valid until their expiry dates or until specific regulatory changes are implemented, the restructuring is expected to introduce new licensing requirements and permit application processes. The newly restructured agencies may eventually mandate the use of new license or permit forms, or require businesses to obtain entirely new licenses or permits based on revised regulations. This can lead to additional administrative burdens and delays for businesses.

### **Recommendations for Businesses**

As Vietnam's political system undergoes this significant transformation, businesses should take the following steps to effectively navigate this period:

- a) Understand the roles and responsibilities of new state agencies to navigate the changing regulatory landscape effectively;
  - b) Regularly review and stay informed about new regulations to ensure compliance and avoid potential penalties; and
  - c) Establish clear and prompt communication with relevant government agencies when carrying out regulatory procedures to avoid unnecessary delays and costs.
-

## CONTACTS



**Tram Ngoc Bich  
Nguyen**

Partner, Corporate and  
Commercial  
Tilleke & Gibbins

**T:** +84 28 6284 5668  
**E:** tram.n@tilleke.com



**Tan Nhat Truong  
Phan**

Associate, Corporate  
and Commercial  
Tilleke & Gibbins

**T:** +84 28 628 45672  
**E:** tan.p@tilleke.com



**Ngan Thuc Nguyen**

Paralegal, Corporate  
and Commercial  
Tilleke & Gibbins

**T:** +84 26 6284 8185  
**E:** thucngan.n  
@tilleke.com

## Technology Legal Update

### A Closer Look at Vietnam's Decree 147 on Internet Services and Online Information

Vietnam's Decree No. 147/2024/ND-CP on the management, provision, and use of internet services and online information (Decree 147) was [issued on November 9, 2024](#), and came into effect on December 25, 2024. Decree 147 represents a more stringently regulated digital landscape in Vietnam, creating challenges not only for offshore service providers offering cross-border services but also for onshore providers. As these new regulations impose stricter requirements, particularly in areas like content control, user authentication, data storage, and service license/notification, companies will need to adapt quickly to maintain compliance and minimize legal risks.

The following are some of the key topics covered by Decree 147.

*[Note: Shortly after the issuance of Decree 147, Vietnam began a [government restructuring process](#), with the aim of streamlining the government by consolidating and eliminating various ministries and agencies. Thus, the decree's references to authorities such as the Authority of Broadcasting and Electronic Information (ABEI) and the Ministry of Information and Communications (MIC) are subject to change.]*

#### a) Cross-Border Information Provision

Cross-border information provision is defined broadly as the provision by overseas organizations and individuals of information and online information content services for service users in Vietnam to access or use. This wide-ranging definition encompasses various types of cross-border services, including social network services, online game services, and app store services. However, cross-border provision of online game services remains prohibited under Decree 147 (see further details below).

Offshore providers of services on a cross-border basis who lease data storage in Vietnam or meet a threshold of 100,000 or more total visits per month from Vietnam for six consecutive months ("regulated cross-border providers") must adhere to stricter requirements. Specifically, they are required to, among other requirements:

1. Notify the relevant authority of their contact information, including the location of the main server providing the service, within 60 days of reaching the total visit threshold;
2. Inspect, monitor, prevent, and remove any content, services, and applications that violate the law within 24 hours from the time of a request from the relevant authority, and within 48 hours of receiving complaints from Vietnamese users regarding content, services, and applications that violate Article 8 of the Cybersecurity Law (which lists a wide range of prohibited acts in cyberspace, such as cyberterrorism, spreading malware, and advertising or trading in banned goods/services);

3. Store personal data of users from Vietnam, such as full name, date of birth, email, and Vietnamese mobile phone number (or ID number), and delete this data when the storage period expires;
4. Provide information of users from Vietnam to the relevant authority upon request for investigation and for law enforcement purposes;
5. Authenticate social network user accounts via users' Vietnamese mobile phone numbers or ID numbers if they do not have Vietnamese mobile phone numbers, or if they use the livestream feature for commercial purposes; and ensuring that only verified accounts can post information (write posts or comments, livestream) and share content on social networks;
6. Classify and display warnings of content that is not suitable for children;
7. Receive and handle complaints from service users;
8. Provide tools for searching and scanning content as requested by the relevant authority; and
9. Report annually to the relevant authority on their service provision to users from Vietnam and on an *ad hoc* basis regarding matters of national security, social order, and emergency upon the authority's request.

Failure to comply with these obligations allows the relevant authority to enforce technical measures to block non-compliant content, services, and applications, as well as impose administrative penalties.

Only cross-border service providers who have notified the relevant authority of their contact information are allowed to provide livestream features or provide revenue-generating activities in any form.

## b) Social Network Services

Regulated offshore social network service providers will be required to meet the obligations outlined above on cross-border information provision.

Onshore social network services, offered by organizations or enterprises with legal status in Vietnam, are categorized as either "high-visitor" or "low-visitor" based on the number of regular visitors. The high-visitor category includes social networks with total monthly visits of 10,000 or more (based on a monthly average over six consecutive months) or with more than 1,000 regular users in a month ("regular" is not further defined). High-visitor onshore social network service providers are required to obtain a license from the relevant authority to operate, while low-visitor providers must obtain a notification confirmation from the authority to provide social network services.

Only **licensed** onshore providers are permitted to provide livestream features or engage in revenue-generating activities of any kind. Therefore, if a low-visitor onshore provider intends to offer livestream features or revenue-generated services, it must apply for a social network service license.

Onshore social network service providers face stricter requirements than regulated offshore social network service providers as they must additionally meet obligations including having at least one server in Vietnam to serve investigations and information provision at the request of the relevant authority, connecting to the monitoring system of the relevant authority for statistics and user access monitoring, and being subject to inspections by the authority.

Within 90 days from the effective date of Decree 147 (i.e., by March 25, 2025), both onshore and regulated offshore social network service providers were required to authenticate the identities of their active users. Additionally, within this same timeline, licensed onshore social network service providers are required to review and report to the relevant authority the number of total visits per month from Vietnam for six consecutive months, as well as the number of regular users per month.

Both onshore and offshore social network service providers must temporarily or permanently block social network accounts, community pages, community groups, and content channels that frequently violate the law. Temporary blocking will be applied at the relevant authority's request when these accounts, community pages/groups, or channels have been found to violate the law at least five times within a 30-day period or at least 10 times within a 90-day period. The temporary block must be implemented within 24 hours of the relevant authority's request and will last from 7 to 30 days, depending on the number and severity of the violations. A permanent block will be enforced when such accounts, community pages/groups, or channels publish illegal content that impacts national security or have previously been temporarily blocked at least three times as per request from the relevant authority.

If onshore social network service providers do not comply with the request of the relevant authority, the authority will suspend the provision of social networking services or revoke the license.

### **c) Online Game Services**

Decree 147 expressly provides that offshore entities providing online game services to users in Vietnam must establish an enterprise in compliance with the decree and with regulations on foreign investment to provide such services. As a result, the cross-border provision of online games remains prohibited.

Online games are still categorized into four types: G1 games have interaction among multiple players via the game server; G2 games only have interaction between players and the game server; G3 games have interaction among multiple players without interaction between players and the game server; and G4 games are downloaded from the internet without interaction among players or between players and the game server.

Enterprises may provide G1 games after obtaining a license to provide G1 game services and a decision on release of a G1 game. Meanwhile, to provide G2, G3, and G4 games, enterprises must obtain a certificate of game service provision and a notification confirmation of G2, G3, or G4 game release. The license to provide G1 game services and certificate of game

service provision for G2, G3 and G4 game services have a 10-year maximum duration while the decision and notification confirmation of game release has a 5-year maximum duration.

Decree 147 explicitly introduces regulations that prohibit the release of online games that feature content and scenarios resembling prizewinning games in casinos or games using images of playing cards. This regulation is designed to prevent transformation of online games into gambling activities in the virtual realm.

The main responsibilities of online game service providers include:

1. Having at least one server in Vietnam to serve the purposes of investigations by the relevant authority and handling of user complaints;
2. Having a website that introduces and provides services, displaying required information such as age-based game classification, rules for handling complaints and disputes, and details about the service provider;
3. Implementing measures to mitigate the negative impacts of each game, including registering, storing, authenticating, and managing player content and information, and ensuring that only players who provide complete and accurate information can participate, and players are warned about the effects of excessive gameplay;
4. Implementing technical measures to manage forums, shared content, and interactions between players;
5. Not advertising online games without a decision on G1 game release or notification confirmation of G2, G3, or G4 game release;
6. Submitting service provision reports regularly every six months and on an *ad hoc* basis when requested by the relevant authority;
7. Being subject to inspections, examinations, and enforcement actions by the relevant authority;
8. Connecting to legitimate payment methods only; and
9. Storing player information for the duration of service use and for six months after a player stops using the service. Providers must also establish a system to connect to the national population database to verify player information upon request by the relevant authority.

d) **App Store Services**

Regulated cross-border app store service providers will be required to meet the obligations outlined above for cross-border information provision. Additionally, they are required to remove any apps that violate the law within 24 hours of receiving a request from the relevant authority; comply with Vietnamese payment regulations; and ensure that any online game service providers offering services to users in Vietnam provide the decision on G1

game release or notification confirmation of G2, G3, G4 game release before uploading their games to the app store.

e) **Telecom, Internet, Web Hosting, Data Center, and Telecom Application Services**

Telecom, internet, web hosting, data center and telecom application service providers are required to report to the relevant authority within 24 hours of self-discovery or receipt of feedback or complaints from users about content, services, and applications that violate Article 8 of the Cybersecurity Law; remove infringing content within 24 hours of request from the relevant authority; and handle requests and complaints about intellectual property in accordance with intellectual property laws. Additionally, they are required to submit annual reports to the relevant authority on data storage rental services provided in Vietnam to foreign entities for providing cross-border information to Vietnamese users, as well as *ad hoc* reports when requested by the relevant authority.

Telecom and internet enterprises must also, among other obligations:

1. Implement necessary technical measures to block access to content, services, and applications that violate the law within 24 hours of receiving a request from the relevant authority, e.g., Department of Cybersecurity and High-Tech Crime Prevention (A05) of the Ministry of Public Security (MPS);
2. Implement measures to monitor, collect, and detect information that violates the law at the request of the relevant authority (for violations of copyright and intellectual property, in compliance with intellectual property law);
3. Provide information and data related to telecom and internet subscribers suspected of violations to enable accurate identification of offenders, upon request from the relevant authority, e.g., A05 under the MPS;
4. Refuse, suspend, or terminate connections to online games without proper licenses or certificates to provide game services or decisions/notification confirmations for game release; and
5. Comply with the relevant authority's requests to coordinate, report, and carry out other measures as requested by the authority.

f) **Public Internet Access Points**

Owners of public internet access points in hotels, restaurants, airports, coffee shops, and other public spaces who offer **paid** internet access services must register as internet agency businesses and sign internet agency contracts, while those offering the services for free are not required to do so.

Internet agents are required to display an "internet agent" sign with their registration number. If the location also serves as a public online gaming point or public internet access point, this information must also be clearly

indicated on the sign. When providing online game services, internet agents also have the responsibilities of an owner of a public online gaming point. Additionally, they must not organize or allow internet users to use computer features at their business location to perform prohibited acts.

---

## CONTACTS



**Giang Thi Huong  
Tran**

Senior Associate,  
Corporate and  
Commercial  
Tilleke & Gibbins

**T:** +84 24 3772 5560  
**E:** [giang.t@tilleke.com](mailto:giang.t@tilleke.com)



**Thao Thu Bui**

Associate, Corporate  
and Commercial  
Tilleke & Gibbins

**T:** +84 24 3772 5532  
**E:** [thao.b@tilleke.com](mailto:thao.b@tilleke.com)

t

# DNA



- Singapore
- Philippines
- Myanmar
- Indonesia
- Cambodia
- Thailand
- Malaysia
- Laos
- Vietnam

[www.drewnetworkasia.com](http://www.drewnetworkasia.com)

[www.linkedin.com/company/drewnetworkasia](https://www.linkedin.com/company/drewnetworkasia)