



ASEAN ROUNDUP



CONTENTS

NO.	COUNTRY	CONTENT	PAGE
1.	Singapore	Singapore High Court on Determining the Location of Cryptoassets - <i>Cheong Jun Yoong v Three Arrows Capital Ltd and others</i> [2024] SGHC 21	4
2.	Singapore	High Court Rejects Employer's Bid to Restrain a Former Employee from Joining a Competitor - <i>Shopee Singapore Pte Ltd v Lim Teck Yong</i> [2024] SGHC 29	8
3.	Malaysia	Federal Court Affirms the Applicability of the "Contract Test" in Constructive Dismissal Cases	12
4.	Malaysia	Industrial Court Upholds the Employer's Policy in Relation to Covid-19 Vaccination	15
5.	Indonesia	Refining Digital Financial Innovation: New OJK Regulation aims to enhance Regulatory Sandbox	18
6.	Cambodia	Cambodia Institutes Steam Energy Permit Requirement	24
7.	Laos	Laos Regulates Management of Foreign Currency from Exports	27
8.	Myanmar	Myanmar Sets Fees for Required Online Retail Business Registration	31
9.	Thailand	Thailand Lays Out New Cybersecurity Standards	34
10.	Vietnam	Vietnam to Conduct First PDPD Compliance Investigation	38



SINGAPORE

DREW & NAPIER LLC

Blockchain & Digital Assets Legal update

Singapore High Court on Determining the Location of Cryptoassets - *Cheong Jun Yoong v Three Arrows Capital Ltd and others* [2024] SGHC 21

Introduction

The recent High Court decision of *Cheong Jun Toong v Three Arrows Capital Ltd and others* [2024] SGHC 21 is notable in that it sets out how the location of a cryptoasset should be determined.

Director Blossom Hing, Associate Director Joshua Chin and Senior Associate Claire Neoh successfully acted for Mr Cheong Jun Yoong, the Claimant in these proceedings.

Background

Three Arrows Capital Ltd (“**Company**”) was incorporated in the British Virgin Islands in 2012. Mr Cheong managed a portfolio of assets in the Company and in November 2019, wanted to formally set up a fund (“**Fund**”). Following a discussion with the Company’s investment manager, the Company created sub-accounts for Mr Cheong within the Company’s main accounts on two cryptocurrency exchanges. The Claimant and investors subscribed for a specially created class of shares and interests and paid for them by transferring cryptocurrencies and fiat currencies into the sub-accounts, which were then used to purchase other assets (“**Assets**”).

Mr Cheong had sole discretion and control over the Fund and had a coworking space for himself and his employees. Any increase in the value of the Assets therefore accrued solely to Mr Cheong and the investors. The Company subsequently set up a workspace which stored cryptocurrency tokens forming part of the Assets. Only Mr Cheong and his representatives could access this platform. Part of the Assets were also stored in Mr Cheong’s cold wallets.

In June 2022, the Company transferred all its rights and interests in the workspace and the Assets in the Company’s sub-accounts to DeFiance Capital Pte Ltd, a company which Mr Cheong incorporated. At this point, a number of Assets were not transferred to Mr Cheong nor DeFiance Capital Pte Ltd. DeFiance Capital Pte Ltd subsequently novated the workspace to DeFiance Ventures Pte Ltd, another company which Mr Cheong incorporated.

The Company was placed under liquidation on 27 June 2022 by a court in the British Virgin Islands (“**BVI Liquidation Proceedings**”). On 9 July 2022, the Singapore High Court recognised the BVI Liquidation Proceedings as a foreign main proceeding. Mr Cheong commenced proceedings in Singapore, claiming that the Assets were held on trust by the Company for the benefit of the investors. The liquidators filed an application the BVI Liquidation Proceedings seeking orders that the Assets were beneficially owned by the Company (“**Parallel BVI Proceedings**”).

On 10 May 2023, the Singapore High Court granted Mr Cheong permission to serve court papers on the Company and its liquidators. Mr Cheong effected service on the Company and its liquidators, and the Company and its liquidators filed an application to set aside the service of court papers.

The High Court's Decision

The High Court dismissed the application by the Company and its liquidators because Mr Cheong had shown that there is a good arguable case that there is sufficient nexus to Singapore, Singapore is the forum conveniens, and that there is a serious question to be tried on the merits of Mr Cheong's claim.

Sufficient nexus to Singapore

The High Court considered para 63(3) of the Supreme Court Practice Directions 2021 and held that Mr Cheong's claim: (a) was made to assert, declare or determine proprietary rights in or over movable property situated in Singapore and, (b) was founded on a cause of action arising in Singapore. There was therefore sufficient nexus to Singapore.

The High Court held that the residence of the person who controls the private key should be treated as the situs of the cryptoasset linked to that private key. On the evidence, the High Court held that DeFiance Ventures Pte Ltd and Mr Cheong controlled the private key to the assets and they were both resident in Singapore.

The High Court also held that the issuance of the shares and interests took place when the Company was headquartered and operating in Singapore.

Singapore was the more appropriate forum

The High Court held that there were several relevant factors which pointed to Singapore being the more appropriate forum. The High Court noted that most of the relevant witnesses are in Singapore and that the relevant documents are also in Singapore.

The High Court considered that the Parallel BVI Proceedings were not significant given the early stage of the proceedings.

There was a serious question to be tried

The High Court held that the evidence supported Mr Cheong's claim.

Commentary

In recent years, there has been a precipitous rise in disputes concerning cryptoassets. Often cross-border in nature, a key consideration which often arises in such disputes is the location of the cryptoassets, not least because of its

impact on a litigant's ability to obtain injunctive relief, and ultimately, a favourable judgment on the merits.

It is against this backdrop that the Singapore High Court's decision of *Cheong Jun Yoong v Three Arrows Capital Ltd and others* [2024] SGHC 21 provides much welcomed clarity on the determination of the location of cryptoassets. Indeed, prior to this decision, the only guidance that could be had was that from the United Kingdom, where differing approaches were adopted:

- a) In *Ion Science v Persons Unknown* (unreported) (21 December 2020), the UK High Court held that the situs of a cryptoasset is the place where the owner of the cryptoasset "*resides or is domiciled*".
- b) In *Lavinia Deborah Osbourne v Persons Unknown* [2022] EWHC 1021, the UK High Court decided that cryptoassets are to be treated as located at the place where the owner is domiciled. In a related case in *Lavinia Deborah Osbourne v Person Unknown Category A* [2023] EWHC 39 (KB), a differently constituted Court reached the same conclusion.
- c) However, in *Tulip Trading Ltd (a Seychelles company) v Van Der Laan* [2022] 2 All ER (Comm) 624 ("**Tulip Trading**"), the UK High Court held that the situs of a cryptoasset is to be tested by reference to residence, rather than domicile. This finding was upheld on appeal: *Tulip Trading Ltd (a Seychelles company) v Bitcoin Association for BSV* [2023] 2 All ER (Comm) 479.
- d) Whether the test is one of residence or domicile can have a material impact on the issue of situs the two are not always the same. In the case of a corporation, the domicile is where the corporation was incorporated, while its residence is where the central management and control of its business is exercised. It is not uncommon for both locations to differ in the context of a company conducting international business as was the case in *Tulip Trading*. In the case of an individual, domicile can only be acquired either (i) by birth or (ii) by the combination of residence and intention to reside permanently or indefinitely in the country of residence. This requirement of an intention to reside can lead to potential uncertainties in the identification of domicile in more difficult cases.

In deciding that the situs of a cryptoasset is to be determined by the residence of the person who controls the private key, the Singapore High Court adopted an approach consistent with the choice of law rules for other intangible properties, in particular choses in action. In the case of choses in action, the courts have kept the idea of control in mind and held that the situs is where the chose in action is properly recoverable or can be enforced (which is often where the defendant resides and can be sued).

Closing Remarks

The location of a cryptoasset has implications on jurisdiction issues, such as determining whether the jurisdiction gateways in para 63(3) of the Supreme Court Practice Directions 2021 have been satisfied and/or whether Singapore is the more appropriate forum to hear a dispute.

It may also have implications on the governing law of a claim (for example, in the context of a proprietary claim governed by the *lex situs*) and on enforcement.

A clear and objective method for determining the location of cryptoassets paves the way for the determination of such issues in future disputes.

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



Blossom Hing

Director, Dispute Resolution and Corporate Restructuring & Workouts
Drew & Napier LLC

T: +65 6531 2494
E: blossom.hing@drewnapier.com



Joshua Chin

Associate Director, Dispute Resolution and Corporate Restructuring & Workouts
Drew & Napier LLC

T: +65 6531 2357
E: joshua.chin@drewnapier.com



Claire Neoh

Senior Associate, Dispute Resolution and Corporate Restructuring & Workouts
Drew & Napier LLC

T: +65 6531 2777
E: claire.neoh@drewnapier.com

Employment & Commercial Litigation Legal Update

High Court Rejects Employer's Bid to Restrain a Former Employee from Joining a Competitor - *Shopee Singapore Pte Ltd v Lim Teck Yong* [2024] SGHC 29

Introduction

The High Court recently dismissed an attempt by Shopee Singapore Pte Ltd ("**Shopee**") to restrain a former employee from accepting employment with a competitor, on the basis that Shopee had failed to prove that its claim against the former employee was not frivolous.

This update discusses the decision of *Shopee Singapore Pte Ltd v Lim Teck Yong* [2024] SGHC 29.

Background

Mr Lim Teck Yong was employed by Shopee on 17 August 2015 and had signed an employee confidentiality agreement ("**Confidentiality Agreement**") and a restrictive covenants agreement ("**RC Agreement**"). Clause 2.3 of the Confidentiality Agreement provides that Mr Lim shall keep all proprietary information confidential unless such disclosure is for the exclusive benefit of the Shopee Group. The RC Agreement also contained a non-solicitation and non-competition clause which, amongst others, prevented Mr Lim from accepting employment with a competitor. Mr Lim left Shopee's employment on 31 August 2023 and commenced employment with ByteDance Pte Ltd ("**ByteDance**") which operates a rival e-commerce platform (ie TikTok Shop) on 11 September 2023.

On 24 November 2023, Shopee commenced proceedings and sought a declaration that clause 2.3 of the Confidentiality Agreement and the non-solicitation and non-competition clause in the RC Agreement (collectively, "**Restraint of Trade Clauses**") are valid and enforceable, and that Mr Lim had breached them, thereby seeking damages.

Shopee also sought interim injunctions to restrain Mr Lim from accepting employment with ByteDance and soliciting Shopee's clients and employees. Shopee alleged that Mr Lim's role in ByteDance is substantially similar to the roles he undertook in Shopee.

Shopee argued that the interim injunctions should be granted as Mr Lim has not shown that he will suffer hardship over and above observing his contractual obligations, and in any event:

- a) there is a serious case to be tried in respect of the validity, enforceability and breach of the Restraint of Trade Clauses; and the balance of convenience lies in favour of granting the interim injunctions.

The High Court's Decision

In *Man Financial (S) Pte Ltd (formerly known as E D & F Man International (S) Pte Ltd) v Wong Bark Chuan David* [2008] 1 SLR(R) 663, the Singapore Court of Appeal held that restraint of trade clauses, particularly those in the context of employment, are prima facie void and unenforceable. This is to give effect to the public policy that frowns upon attempts to unreasonably proscribe freedom of trade.

The High Court held that an applicant seeking an interim injunction in respect of a restraint of trade clause must show:

- a) a serious question to be tried that the restraint of trade clause is valid and enforceable, namely that it protects a legitimate proprietary interest and that it is reasonable in the interests of the parties and the public;
- b) a serious question to be tried (with a real prospect of success) that a restraint of trade clause has been breached; and
- c) if there are serious questions to be tried that the balance of convenience lies in favour of the granting the interim injunction.

According to the High Court, Shopee failed to demonstrate that the non-competition restriction covers a legitimate proprietary interest over and above the protection of trade connections. The confidential information that Shopee sought to protect was set out along fairly generic categories, and Shopee's failure to point to any specific confidential information affected the geographical scope of the restraint that Shopee sought in the non-competition restriction. In effect, Shopee was seeking to have Mr Lim restrained from working for any of Shopee's competitors who had been in all the markets where Shopee was operating, even though Mr Lim was not even working in or had no responsibilities for those markets. The High Court therefore doubted that it could be said that there was a serious question if this would be regarded as reasonable as between the parties or reasonable in the interest of the public.

The High Court further noted that Mr Lim had stated on affidavit that he had not and would not breach the confidentiality restrictions or the non-solicitation restrictions, and therefore found that Shopee had not, on its bare assertions alone, shown a serious case to be tried that the non-solicitation restrictions had been or were about to be breached by Mr Lim.

Commentary

Restraint of trade clauses are not uncommon in employment contracts in Singapore. Typically, they seek to restrain employees from working for a competitor or within the same industry for a period of time after leaving their employment. Such clauses, by their very nature, impinge on an employee's right and freedom to work.

This case illustrates the challenges and pitfalls employers can face when enforcing restraint of trade clauses against employees. In particular, the case highlights that an employer seeking an injunction to prevent an employee from working for a competitor will need to come prepared with evidence that its

legitimate proprietary interests are at risk of being compromised. Given that questions of validity and enforceability of restraint of trade clauses are ultimately fact-dependent, legal advice should be sought before employers rely on such clauses to restrain their employees.

Finally, it is worth noting that the Ministry of Manpower has announced that it will soon develop guidelines regarding non-compete clauses in employment contracts. Such guidelines will no doubt provide further guidance for both employers and employees on the application of such clauses.

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



Chia Voon Jiet

Director, Dispute
Resolution
Co-Head, Investigations
Drew & Napier LLC

T: +65 6531 2397

E: voonjiet.chia
@drewnapier.com



MALAYSIA

SHEARN DELAMORE & CO.

Employment & Administrative Legal Update

Federal Court Affirms the Applicability of the “Contract Test” in Constructive Dismissal Cases

In the case of **Tan Lay Peng (in her capacity as the administratrix of the estate of Tan Leong Huat) v. RHB Bank Berhad (Civil Appeal No.01(f)-10-04/2023(P))**, which was decided on 9 February 2024, the Federal Court unanimously affirmed the “*contract test*” as the appropriate test for determining a constructive dismissal case.

A former employee of RHB Bank Berhad (“**the Bank/Respondent**”), Tan Leong Huat (“**Mr. Tan/Appellant**”), was employed by the Bank as its Operations Head, Thailand Operations in Bangkok, the sole branch of the Bank at the material time.

In November 2013, the Bank opened its second branch in Sri Racha which was placed under the supervision of Mr. Tan. In June 2014, the Bank appointed Ms. Marina Chin Yoke Fong as the Head of Thailand Operations to oversee the operations of the Bangkok, Sri Racha, and the intended Ayutthaya branches.

In 2014, the Bank issued a transfer order for Mr. Tan to assume the role of Branch Manager of the Ayutthaya branch. The transfer order stipulated that his assignment is for a period of nine months. Mr. Tan complied with the transfer order and the Ayutthaya branch was opened in November 2014.

Subsequently, the Bank appointed a Thai national, Ms. Irin Chanonthiensink, as the Ayutthaya Branch Manager. In the circumstances, the Bank issued a transfer order for the transfer of Mr. Tan to the International Infrastructure, PMO and Operation Support, Group International Business in Malaysia with effect from 1 March 2015. Mr. Tan objected to his repatriation to Malaysia, refused to report for duty and pleaded constructive dismissal.

The Industrial Court found in favour of Mr. Tan and awarded him the sum of RM216,840 as compensation in lieu of reinstatement. The Bank’s application for judicial review was dismissed by the High Court. However, on appeal to the Court of Appeal, the Court of Appeal decided that the Industrial Court had applied the wrong test in determining whether Mr. Tan was constructively dismissed, giving rise to the appeal before the Federal Court.

The question of law before the Federal Court was as follows:

“Is there a difference in the contract test or reasonableness test in light of major developments in industrial jurisprudence?”

In answering the foregoing question, the Appellant submitted that despite the differences between the contract and reasonableness test, both tests have similar characteristics and/or approaches, and as such they can be used and/or must be used interchangeably when determining a claim of constructive dismissal.

The Respondent submitted that the sole and relevant test for constructive dismissal is the contract test and not the reasonableness test. The

Respondent further submitted that the development of the implied duty of trust and confidence does not displace the contract test with any other test including the reasonableness test and that the unreasonable conduct of an employer is insufficient to sustain a claim of constructive dismissal. The Respondent contended that Mr. Tan's repatriation was in accordance with the transfer clause in his contract of employment.

The Federal Court ruled in favour of the Respondent and emphasised that the applicable test for constructive dismissal cases is the contract test. In arriving at its decision, the Federal Court considered the current position of the law on constructive dismissal in Malaysia and other jurisdictions (England, Singapore, Australia and Canada), and concluded that the contract test in determining constructive dismissal is good law and there is no reason to depart from the said position.

The Federal Court resoundingly rejected the Appellant's contention that there is a need to consider the breach of reasonableness, fairness, good faith and bona fide act of the employer's action in deciding whether there was any fundamental breach in the terms of the employment.

Whilst the reasonableness of the employer's conduct can be a factor to be taken into consideration in determining whether there is any fundamental breach of the contract of employment by the employer, this is insufficient in establishing constructive dismissal. The Federal Court held that to use the reasonableness test as the legal requirement or interchangeably with the contract test would only entail uncertainty and confusion in industrial relations.

The Federal Court's decision is an important, sensible and timely reminder of the test to be adopted by the Courts in Malaysia when assessing a claim of constructive dismissal.

The Bank was represented by N. Sivabalah and Jamie Goh.

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

For further information about this article or employment and administrative law matters in general, please contact:

CONTACTS



N. Sivabalah

Partner, Employment &
Administrative Law
Shearn Delamore & Co.

T: +603 2027 2866
E: sivabalah
@shearndelamore.com



Jamie Goh

Partner, Employment &
Administrative Law
Shearn Delamore & Co.

T: +603 2027 2731
E: jamie.goh
@shearndelamore.com

Employment & Administrative Legal Update

Industrial Court Upholds the Employer's Policy in Relation to Covid-19 Vaccination

In the recent case of **Mazuna Begum binti Kadir Mira v Malaysia Airlines Berhad** [Award No. 196 of 2024], which was handed down on 5 February 2024, the Industrial Court evaluated the validity of Malaysia Airline's Berhad policy relating to Covid-19 vaccination for its employees.

The Claimant was employed as a Cabin Crew with the company and her dismissal was based on the charge of insubordination due to her refusal to comply with the company's policy (the "**MAG Vaccination Policy**"), which mandated all employees based in Malaysia to be vaccinated unless there were valid medical reasons for exemption.

The company argued the dismissal was with just cause or excuse as it had a duty to ensure a safe working environment for all its employees and customers, while the Claimant alleged that she had concerns about being vaccinated and had a right to refuse the vaccine, as well as alleging discrimination and victimization. The Claimant also relied on the fact that the Government of Malaysia did not mandate citizens to take the Covid-19 vaccine.

The Industrial Court found in favour of Malaysia Airlines Berhad and emphasised that the company's policy aligns with the national COVID-19 Immunisation Programme which is aimed at safeguarding the welfare of all citizens. Therefore, both the national programme and the company's policy should not be undermined by the refusal of individuals, including the Claimant, to participate in the vaccination drive. In this regard, the Industrial Court emphasised that private or sectional interests which are inconsistent with the larger and greater interest of the nation or public must give way to the latter. The Industrial Court accordingly found that the Company had proved on the balance of probabilities that the Claimant was dismissed from her employment with just cause or excuse and dismissed the Claimant's claim.

The instant decision is pivotal as represents the Industrial Court's attempt to balance the obligation of an employer to provide a safe working environment for its employees and the individual rights of employees to refuse to accept the Covid-19 vaccine. The decision also sets a precedent for other factually similar cases relating to the Covid-19 vaccination that are currently pending before the courts.

Malaysia Airlines Berhad was represented by Vijayan Venugopal during the court proceedings.

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

For further information about this article or employment and administrative law matters in general, please contact:

CONTACT



Vijayan Venugopal

Head, Employment &
Administrative Law
Shearn Delamore & Co.

T: +603 2027 2874

E: vijayan@shearndelamore.com



INDONESIA

MAKARIM & TAIRA S.

Financial Services Regulation Legal Update

Refining Digital Financial Innovation: New OJK Regulation aims to enhance Regulatory Sandbox

Almost six years ago, Indonesia's Financial Services Authority (*Otoritas Jasa Keuangan* – “**OJK**”) introduced a new regulation on digital financial innovation (*inovasi keuangan digital* – “**IKD**”) in financial services (“**POJK 13/2018**”) (see our Advisory on the OJK regulatory sandbox issued in August 2018). The concept of IKD was further developed with the enactment of Law No. 4 of 2023 on Financial Sector Development and Reinforcement (“**P2SK Law**”) and is now known as technology innovation in the financial sector (*inovasi teknologi sektor keuangan* – “**ITSK**”).

Following the enactment of the P2SK Law, the OJK has introduced a new regulation, OJK Regulation No. 3 of 2024 on the Organisation of Financial Sector Technology Innovation (“**POJK 3/2024**”), aimed at further regulating ITSK. This regulation supersedes POJK 13/2018, which previously governed IKD. The OJK has enhanced several aspects of POJK 13/2018 through POJK 3/2024, including the addition of eligibility criteria, the introduction of test plan requirements, and the establishment of procedures for determining results and exiting the sandbox.

ITSK Development

Since its introduction in 2018, the concept of IKD/ITSK has undergone significant development. According to the OJK's routine official publication on IKD/ITSK, as of November 2023, at least 97 IKD/ITSK organisers (“**Organiser**”) had been recorded by the OJK and 4 of them have received “Recommended” status from the OJK. These Organisers cover 14 types of IKD/ITSK clusters, including innovative credit scoring, aggregators, transaction authentication, E-KYC, wealth tech, insurance tech, and insurance hubs.

POJK 3/2024 vs. POJK 13/2018: What's new in POJK 3/2024?

The provisions of POJK 3/2024 on ITSK mostly mirror those of POJK 13/2018. Under POJK 3/2024, Organisers are required to comply with OJK licensing requirements before they commence their business activities. Below are a few of the main differences and updates in the new regulation.

A. ITSK Organisers

Organisers are parties who organise a technology-based innovation that impacts products, activities, services, and business models in the digital financial ecosystem. They can be either:

1. Financial services institutions (*Lembaga Jasa Keuangan*); or
2. Other parties conducting activities in the financial sector in accordance with the prevailing laws and regulations.

An ITSK organiser must be a limited liability company or other legal entity recognized under the prevailing laws and regulations.

B. ITSK Scope

Under POJK 3/2024, there are two main differences in the scope of ITSK activities compared to IKD.

First, the scope of ITSK, that falls under the authority and supervision of the OJK, has been expanded to include activities related to crypto assets, which previously came under the authority of the Commodity Futures Trading Supervisory Agency (*Badan Pengawas Perdagangan Berjangka Komoditi – BAPPEBTI*).

Second, insurance activities, previously covered in POJK 13/2018, are now not specifically included in the scope of ITSK activities in POJK 3/2024.

The scope of ITSK activities related to digital financial assets under POJK 3/2024 are now as follows:

- the settlement of securities transactions;
- raising capital;
- investment management;
- risk management;
- the collection and distribution of funds;
- providing market support;
- activities related to digital financial assets, including crypto assets; and
- other digital financial services activities.

C. Regulatory Sandbox Process

POJK 3/2024 uses a similar mechanism for Organisers to participate in the sandbox process. Under the previous regulation (POJK 13/2018), participation in the regulatory sandbox involved the use of the recordation mechanism within the OJK system. Organisers would initially submit a recordation application to the OJK along with the required documents. Following the recording process, the OJK would determine which Organisers could participate in the regulatory sandbox, provided they fulfilled the minimum criteria.

Similarly, POJK 3/2024 requires Organisers to submit an application to join the regulatory sandbox. The difference in POJK 3/2024 is that this 'application stage' no longer recognizes the recordation step which was introduced by POJK 13/2018. Now, Organisers who wish to undergo the regulatory sandbox merely apply to become a 'participant' in the OJK regulatory sandbox. This application should include an application form, test plan, and other supporting documents. The OJK will then evaluate the test plan of potential participants of the regulatory sandbox. If the OJK deems that improvements are necessary to the test plan, participants must make these improvements and resubmit the revised test plan to the OJK.

In brief, under POJK 3/2024, the updated regulatory sandbox process is as follows:

1. Submission of application documents to become a participant, including the application form, test plan, and supporting documents.
2. Approval by the OJK to participate in the regulatory sandbox.
3. Conducting the regulatory sandbox process, with a maximum duration of one year.
4. Evaluation of the sandbox process results, determining a pass or fail outcome.
5. In the event of a failure result, Organisers must cease all business activities and implement their exit policy program.
6. If the sandbox result is a pass, Organisers must apply for a business license from the OJK.

D. Test Plan

Before becoming a participant in the sandbox process, Organisers must submit a test plan, which should include, among other details:

- An explanation of the product innovation, activities, services, or business models to be tested and developed.
- Identification of potential risks associated with the innovation of products, activities, services, or business models.
- Implementation plan for mitigating potential risks.
- Limitations of the implementation of the testing and development of innovation, including the testing period required, target consumer profiles, number of consumers, testing and development partners, number of transactions, and other measurable limitations.
- Consumer protection framework, including consumer complaint services and compensation mechanisms.
- Financial readiness and resources available to conduct the testing and development of the innovation.
- Exit and transition policies if the tested and developed innovation cannot continue after the sandbox process.
- Testing and development scenarios for the innovative products, activities, services, or business models to be tested and developed.
- Key performance indicators for the testing and development scenarios.

This test plan requirement is newly introduced in POJK 3/2024 and is a more detailed version of the business plan required under the previous POJK 13/2018 regime.

E. Eligibility Criteria

POJK 3/2024 introduces a set of criteria used to assess whether an Organiser may participate in the regulatory sandbox. These 'Eligibility Criteria' include:

- Innovations with a scope of coverage in the financial services sector, to be used by consumers, partners, or the public in Indonesia.
- Innovations with an element of novelty or a significant differentiating element from existing practices in the financial sector.

- Innovations that provide benefits, improve services, and add value to consumers, the public, or the financial sector ecosystem.
- Innovations that are ready for testing and development.
- Innovations that require trial and development support and have not been regulated or supervised previously under financial sector regulations.
- Other criteria determined by the OJK.

These criteria are established to guide the OJK in determining the eligibility of Organisers' innovations for participation in the sandbox process. Based on these criteria, the OJK will either approve or reject an Organiser's application. Further provisions regarding eligibility criteria and approval will be issued by the OJK.

ITSK Sandbox Results

The mechanism for determining sandbox results is different under POJK 3/2024 compared to 13/POJK.02/2018. Under POJK 13/2018, the regulatory sandbox results for the Organiser were categorized as (i) recommended, (ii) improvement, or (iii) not recommended. Meanwhile, POJK 3/2024 specifies that the sandbox results are simply categorized as pass or fail, without providing Organisers an opportunity to improve their test results.

Under POJK 3/2024, after conducting tests and developing innovations in the sandbox, an Organiser must submit a final report on the implementation of the innovation testing and the development of its business. Subsequently, the OJK will evaluate the sandbox results and decide whether the Organiser has passed or failed. If the Organiser has passed the sandbox testing, it must apply for a business license from the OJK within the effective term of the approval letter. This approval letter is not a business license for the Organiser to carry out commercial activities. However, the licensing process is yet to be regulated under POJK 3/2024, which only stipulates that the business licensing process will follow OJK regulations on licensing and supervision for each type of ITSK.

Reporting Obligations

POJK 3/2024 sets out new reporting obligations for organisers registered or licensed by the OJK. The reporting obligations consists of two reports:

- Monthly Report: Organisers must submit a monthly report to the OJK within 10 working days after the reporting period ends.
- Annual Report: An annual report must be submitted no later than April 30 of the following year.

Other Matters and Transitional Provisions

- Organisers registered or licensed by the OJK is required to maintain both a data center and data recovery centers in Indonesia.
- Organisers Undergoing registration application and participants of the regulatory sandbox under POJK 13/2018 after the issuance of POJK 13/2018 are given one of three statuses: (a) recommended with the obligation to

register or obtain a license from the OJK; (b) recommended without the obligation to register or obtain a license from the OJK; or (c) not recommended. This must be completed within six months from the effective date of POJK 3/2024.

- The enactment of POJK 3/2024 revokes POJK 13/2018, along with all of its implementing regulations.

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



Maria Sagrado

Managing Partner
Makarim & Taira S.

T: +6221 5080 8300
E: maria.sagrado@makarim.com



Mawira A. Sudarmadi

Associate
Makarim & Taira S.

T: +6221 5080 8300
E: Mawira.Sudarmadi@makarim.com



M. Alfitras Tavares

Associate
Makarim & Taira S.

T: +6221 5080 8300
E: Alfitras.Tavares@makarim.com

A faint, light-colored map of Southeast Asia is visible in the background, showing the outlines of Cambodia, Laos, Vietnam, Thailand, Malaysia, and Indonesia. The map is rendered in a low-poly, geometric style.

CAMBODIA

TILLEKE & GIBBINS

Energy Legal Update

Cambodia Institutes Steam Energy Permit Requirement

On November 4, 2021, Cambodia's Ministry of Mines and Energy (MME) issued a Prakas No. 0305 on Management of the Steam Energy Subsector within the Energy Sector. The prakas aims to regulate steam energy operations, and requires companies wishing to develop, build, install, or operate steam energy to apply for a steam energy license.

As this is the first prakas regulating steam energy operations in Cambodia, all relevant companies operating in steam energy must apply for a steam energy license with the MME.

Prakas 0305 discusses permits for three types of activities:

- **Development, Construction, Installation, and Operation of Steam Energy.** Companies wishing to develop, build, install, and operate steam energy production facilities must first apply for a permit from the MME.
- **Steam Energy Service Provision.** Companies wishing to develop, build, install, and operate steam energy for the purpose of supplying steam energy to consumers must apply for a permit for steam energy service provider in addition to a permit for development, construction, installation, and operation of steam energy.
- **Two-in-One Steam Energy and Electricity Production.** Companies wishing to develop and operate both steam energy and electricity production activities must also apply for a permit for two-in-one steam energy and electricity production.

Companies operating without the necessary permits are subject to a daily fine of KHR 400,000–4,000,000 (approx. USD 100–1,000). In addition, they may face other penalties, including:

- An order to halt business activities;
- Permit suspension;
- Permit revocation;
- Judicial action; and
- Other legal measures as the MME deems fit.

For more information on regulations and requirements for steam energy licenses in Cambodia, please contact Tilleke & Gibbins at cambodia@tilleke.com.

CONTACT



Nitikar Nith

Associate, Corporate
and Commercial
Tilleke & Gibbins

T: +855 23 964 210

E: nitikar.n@tilleke.com



LAOS

TILLEKE & GIBBINS

**Foreign
Currency
Management
Legal Update**

Laos Regulates Management of Foreign Currency from Exports

On March 7, 2024, Laos moved to regulate the management of foreign-currency income from the exportation of goods and services. Effective March 29, 2024, Decision No. 333 (formally the Decision on Management of Income in Foreign Currency from Exportation of Goods and Services No. 333/BOL) from the Bank of Lao PDR (BOL) aims to incentivize the inflow of such foreign currency into Laos and its sale to licensed commercial banks.

Decision No. 333 sets minimum required proportions for importing income in foreign currency derived from the exportation of goods and services, as well as the timeframe for doing so. It also stipulates the requirements for selling such foreign currency to commercial banks in Laos and the minimum proportions that must be sold.

Importing Foreign-Currency Income

Exporters must receive payments from abroad via bank transfer into a dedicated bank account designated for import-export business activities within the timeline specified in the sale-purchase agreement, but not exceeding 180 days from the date of export. Each sector must import income in foreign currency into the Lao PDR according to the minimum proportion of currency to be imported, and it must be done within the required timeframes, as specified in the table below.

Sector	Minimum Proportion to Be Imported	Timeframe (from Date of Export)
Mining	85%	Within 90 days
Services	80%	Within 60 days
Agriculture	75%	Within 60 days
Electricity	20%	Within 180 days
Other	70%	Within 90 days

The ratios and timeframes are subject to change depending on the circumstances. If exporters cannot comply with the required ratio and timeline, exporters must provide relevant explanatory documents for the BOL’s consideration.

Selling Foreign-Currency Income

Exporters of goods and services must sell at least the minimum required proportion of their foreign-currency income (see table below) to a commercial bank in Laos. This foreign currency exchange must occur within three working days of receiving the foreign currency into the dedicated bank account in Laos. The selling rate will be determined by the prevailing rate of the commercial bank on the day of the transaction.

Sector	Minimum Proportion to Be Sold
Mining	35%
Agriculture	30%
Electricity	20%
Services	20%
Other Sectors	20%

In conducting these transactions, commercial banks are required to carefully consider and manage their reserves and overall liquidity to ensure that they can meet public demand.

If an exporter does not sell at least the minimum required amount of foreign currency within three working days, the relevant commercial bank must proceed with the minimum required exchange and notify the exporter that they are doing so.

These requirements do not apply to re-exporters, such as importers of unprocessed raw materials for re-export to other countries, as determined by the Department of Foreign Currency Management (DFCM).

After selling the minimum required amount to a commercial bank, the remaining foreign-currency income must be used for foreign-currency exchange purposes, such as payments to parties in foreign countries, fulfilling obligations to the state, and so on.

Exporters can sell foreign currency to the BOL by notifying it of the need to sell the foreign currency to the DFCM in the BOL, after which they can sell the currency to the BOL through a commercial bank.

Registration

Decision No. 333 requires service exporters to register as importers and exporters to bring in income generated from exporting services. Although it doesn't specify the types of service businesses that need to register, a March 2024 notice from the Ministry of Industry and Commerce offers examples of such businesses, including those in international transport, insurance, tourism and hotels, construction, and consulting.

Violations

First-time violations of Decision No. 333 that do not cause damage are subject to training on the importance of complying with Lao law or a warning. If the violation persists after the training or warning, the violator will face suspension of its ability to export goods and services.

For more information on Decision No. 333, or on any aspect of foreign currency management in Laos, please contact Tilleke & Gibbins at lao@tilleke.com.

CONTACT



Naiyane Xaechao

Associate, Corporate
and Commercial
Tilleke & Gibbins

T: +856 21 262 355

E: naiyane.x@tilleke.com



MYANMAR

TILLEKE & GIBBINS

Business Registration Legal Update

Myanmar Sets Fees for Required Online Retail Business Registration

Myanmar's Ministry of Commerce (MOC) has released updated information regarding the registration fees for online retail businesses. The fees and criteria, which are included in the MOC's Export/Import Newsletter No. 17/2023 dated December 28, 2023, are laid out below.

Registration Fees

The official registration fees vary depending on the applicant type:

- Companies or other commercial organisations: MMK 70,000 (approx. USD 33.5) for registration and renewal; MMK 3,000 (approx. USD 1.5) for each amendment.
- Small and medium enterprises (SMEs): MMK 50,000 (approx. USD 24) for registration and renewal; MMK 3,000 (approx. USD 1.5) for each amendment.
- Individual applicants: 30,000 MMK (approx. USD 14.5) for registration and renewal; MMK 3,000 (approx. USD 1.5) for each amendment.

Validity Period

Registrations approved from January 1, 2024, will be valid for two years from the date of grant.

The [requirement for online retail businesses to register their operations](#) was announced in July 2023. Based on statements from the MOC, online retail businesses need to complete their registration by late January 2024 to avoid potential enforcement actions. Regarding SMEs, the MOC will also evaluate their SME registration certificate issued by the Agency Office under the Small and Medium Enterprises Development Law 2015.

For assistance completing the registration process, or for more details on any aspect of online retail operations in Myanmar, contact Tilleke & Gibbins at myanmar@tilleke.com.

CONTACTS



Yuwadee Thean-Ngarm

Partner and Director,
Intellectual Property,
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



THAILAND

TILLEKE & GIBBINS

Cybersecurity Legal Update

Thailand Lays Out New Cybersecurity Standards

Thailand's National Cyber Security Committee (NCSC) released three notifications under the Cybersecurity Act on January 18, 2024, setting cybersecurity-related requirements for key organizations and assets. While one of these notifications already took effect, the two most notable will take effect on January 18, 2025 (i.e., one year from their publication in the *Government Gazette*).

These two are the NCSC Notification Re: Standards for Defining the Security Category for Data or Information Systems B.E. 2566 (2023) ("Notification on Security Category") and the NCSC Notification Re: Minimum Standards for Data and Information Systems B.E. 2566 (2023) ("Notification on Minimum Standards").

These notifications apply to:

- State agencies;
- Supervising or regulating organizations (i.e., state organizations, private organizations, or persons designated by law to regulate or supervise the affairs of state organizations or critical information infrastructure organizations); and
- Critical information infrastructure organizations (i.e., organizations related to or providing national security, significant public services, banking and finance, information technologies and telecommunications, transportation and logistics, energy and public utilities, and public health).

Collectively these are defined as "Organizations" under the notifications.

Notification on Security Category

The Notification on Security Category sets forth risk-based security classifications—or "security categories"—for Organizations' data or information systems.

For security category assessment purposes, Organizations are required to perform a self-assessment of their data or information systems based on three key security objectives: confidentiality, integrity, and availability. Each of these objectives is further categorized into three risk levels (low, medium, and high), taking into account the assessment of potential impact in the following areas:

- Organizations' financial value or reputation;
- Organizations' number of service users;
- Organizations' ability to perform their duties; and
- State stability or public order.

The risk levels for the three objectives are determined by considering whether there are "minimal," "severe," or "serious severe" effects, as described below:

- Confidentiality (not including data classified as "secret," which follows different criteria): The effects of unauthorized disclosure of data on Organizations' reputation and financial value;

- Integrity: The effects of unauthorized alteration or destruction of data on Organizations’ performance; and
- Availability: The effects of inability to access or use the data or information system on Organizations’ performance.

If their systems handle different types of data, Organizations must assess each type and set the security category based on the highest risk level identified.

The security category should be reviewed at least once every three years, with the results properly recorded.

Notification on Minimum Standards

Once the security category is determined, Organizations are responsible for applying the minimum cybersecurity measures stipulated in the Notification on Minimum Standards. These measures are outlined in the table below, which indicates the items that are required for minimum cybersecurity measures under each security category.

Minimum Cybersecurity Measures	Security Category		
	Low	Medium	High
Guideline Requirement			
Cybersecurity audit plan		•	•
Cybersecurity risk assessment	•	•	•
Incident response plan	•	•	•
Cybersecurity Standard Framework			
1. Risk Identification			
Asset management	•	•	•
Risk assessment and risk management strategy	•	•	•
Vulnerability assessment and penetration testing			•
Third-party management			•
2. Risk Protection			
Access control	•	•	•
System hardening	•	•	•
Remote connection		•	•
Removable storage media		•	•
Cybersecurity awareness	•	•	•
Information sharing			•
3. Risk Detection			
Cyber threat detection and monitoring	•	•	•
4. Risk Response			
Cybersecurity incident response plan	•	•	•
Crisis communication plan	•	•	•
Cybersecurity exercise	•	•	•
5. Recovery			
Cybersecurity resilience and recovery			•

For more information on compliance with these notifications under the Cybersecurity Act, or on any aspect of cybersecurity in Thailand, please contact:

CONTACTS



**Athistha (Nop)
Chitranukroh**

Partner, Corporate and
Commercial
Tilleke & Gibbins

T: +66 2056 5600
E: nop.c@tilleke.com



**Nopparat
Lalitkomon**

Partner, Corporate and
Commercial
Tilleke & Gibbins

T: +66 2056 5646
E: nopparat.l@tilleke.com



**Napassorn
Lertussavavivat**

Associate, Corporate and
Commercial
Tilleke & Gibbins

T: +66 2056 5662
E: napassorn@tilleke.com



Rada Lamsam

Associate, Corporate
and Commercial
Tilleke & Gibbins

T: +66 2056 5713
E: rada.l@tilleke.com

A large, faint, light green map of Southeast Asia and Oceania serves as the background for the page. The map shows the outlines of Vietnam, Laos, Cambodia, Thailand, Malaysia, Indonesia, and the Philippines.

VIETNAM

TILLEKE & GIBBINS

Data Protection Legal Update

Vietnam to Conduct First PDPD Compliance Investigation

Last year, the government of Vietnam issued the Personal Data Protection Decree (PDPD), which took effect on July 1, 2023. The Department of Cybersecurity and High-Tech Crime Prevention and Control (referred to as “A05”) under the Ministry of Public Security (MPS) is tasked with implementing and enforcing the requirements under the PDPD. While a decree on sanctioning provisions for noncompliance with the PDPD is still pending issuance, further movements from the MPS/A05 indicate that it aims to start conducting its first inspections into PDPD compliance.

This is the first time that companies and government agencies have been officially questioned by the MPS about their compliance with the PDPD. The purposes of this inspection program are (1) to evaluate the compliance status of a group of selected companies and government agencies and to understand challenges in complying with the PDPD requirements; (2) to propose sanctions for noncompliance; and (3) to collect information and comments for the development of the upcoming Personal Data Protection Law—not to spot noncompliance with the PDPD specifically.

This round of inspection includes a number of companies in 14 sectors (including e-commerce, aviation, telecom, banking and finance, intermediary payment, insurance, gaming, education, healthcare, real estate, data processing services, ride hailing, etc.). The companies targeted by this inspection program must: (1) submit a report on compliance to the MPS/A05 by May 30, 2024 (this report is different from the data protection impact assessment (DPIA)/transfer impact assessment (TIA) submission requirements); and (2) coordinate with the MPS/A05 on any further investigation actions from June to August 2024. The inspection results will be available by September 2024.

Key information to be reported includes, among others: (1) a description of the activities and measures carried out to implement the PDPD (such as protecting data subjects’ rights, performing administrative procedures, preventing violations, etc.) and their implementation results in practice; (2) assessment and analysis of the shortcomings and reasons, and the lessons learned; (3) a forecast of violations of data privacy law; and (4) recommendations and solutions to overcome the challenges in complying with the PDPD, including specific suggested contents to be included in the draft Personal Data Protection Law.

Due to the absence of the decree on sanctioning, it remains to be seen if and how the MPS/A05 will impose sanctions on companies that have not yet fully complied with the obligations under the PDPD, especially those related to DPIA/TIA submissions. Nevertheless, this is a good time for companies that have not complied with the PDPD to quickly fulfill their obligations under the PDPD before they are subject to the next round of investigation and/or enforcement.

For more information on the Personal data Protection Decree (PDPD), or on any aspect of cybersecurity in Vietnam, please contact:

CONTACTS



**Waewpen
Piemwichai**

Counsel, Corporate and
Commercial
Tilleke & Gibbins

T: +84 24 3772 5618
E: waewpen.p
@tilleke.com



Anh Hoai Nguyen

Senior Associate,
Corporate and
Commercial
Tilleke & Gibbins

T: +84 24 3772 5596
E: hoaianh.n
@tilleke.com



Thao Thu Bui

Associate, Corporate
and Commercial
Tilleke & Gibbins

T: +84 24 3772 5532
E: thao.b@tilleke.com



Mélynda Maheux

Associate, Corporate
and Commercial
Tilleke & Gibbins

T: +84 24 3772 5682
E: melynda.m
@tilleke.com

DNA



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

www.drewnetworkasia.com

www.linkedin.com/company/drewnetworkasia