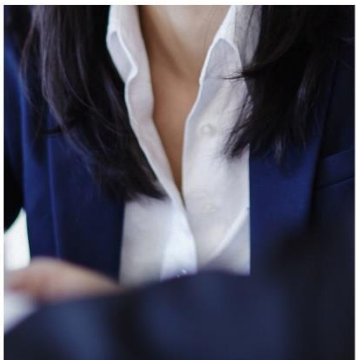
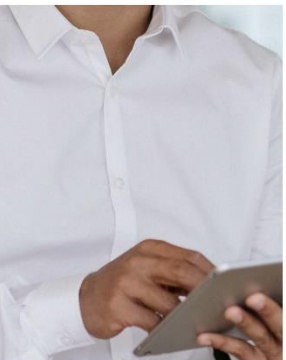
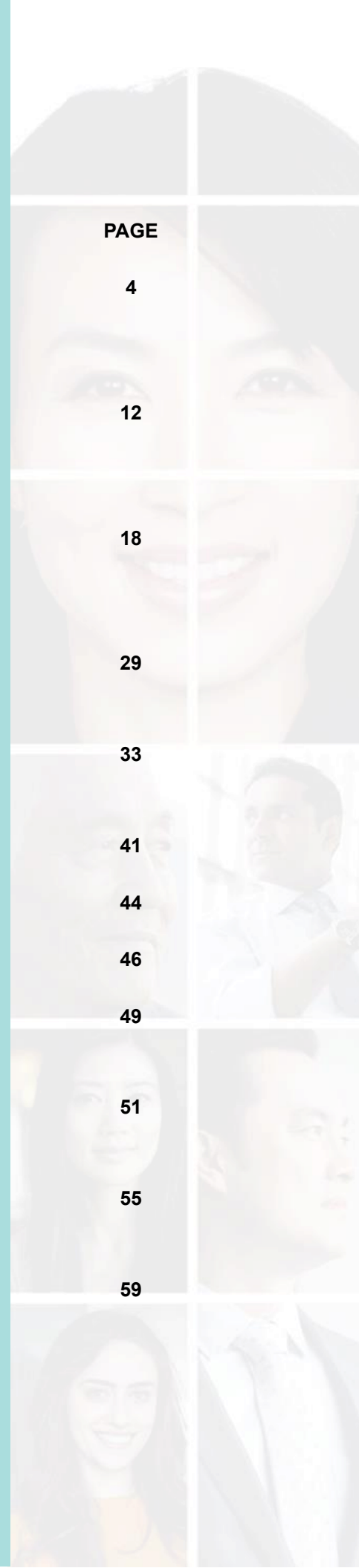


ASEAN ROUNDUP



CONTENTS

NO.	COUNTRY	CONTENT	PAGE
1	Singapore	Personal Data Protection Commission Clarifies Personal Data Protection Act Penalty Framework in Marina Bay Sands Decision	4
2	Singapore	Court Upholds Will — Disinherited Wife’s Challenge Fails; Half-Sister Inherits Estate <i>XAT v XAU and another</i> [2025] SGHCF 4	12
3	Indonesia	Indonesia Simplifies Market Entry, Strengthens Compliance — Insights from Head of BKPM Regulation 5/2025	18
4	Malaysia	Industrial Court Upholds Dismissal over Verbal Sexual Harassment	29
5	Cambodia	Not So Fast: Scaling Back DEI May Violate Local Laws in Southeast Asia	33
6	Laos	Laos Introduces Online Arrival Registration System	41
7	Myanmar	Myanmar Affirms Cryptocurrency Controls	44
8	Myanmar	Myanmar Cybersecurity Law Takes Effect	46
9	Thailand	Thailand Expands Family Leave Rights and Strengthens Worker Protections	49
10	Thailand	Thailand to Remove Import Duty Exemption for Low-Value Goods	51
11	Vietnam	The IP Puzzle of AI-Generated Songs: Protection, Responsibility, and the Future of Music Law	55
12	Vietnam	Vietnam’s New Personal Data Protection Law: A Closer Look	59





SINGAPORE

DREW & NAPIER LLC

Data Protection, Privacy and Cybersecurity Legal update

Personal Data Protection Commission clarifies Personal Data Protection Act penalty framework in Marina Bay Sands decision

Facts of this Case

Marina Bay Sands (“**MBS**”) is an integrated resort operator which runs, among other things, two membership programmes: Sands Rewards Lifestyle (“**SRL**”) and ArtScience Friend (“**ASF**”). SRL members that were visitors of the ArtScience Museum operated by MBS could join the ASF membership programme to access additional benefits. As part of these two programmes, MBS collected the personal data of approximately 1.9 million individuals.

Between 19 and 20 October 2023, a threat actor gained access to six ASF accounts using a technique known as password spraying (i.e. where the same password was attempted to be used to login to many SRL and ASF accounts until access was obtained to one or more accounts). Due to MBS’ password policy at the time, all the default SRL/ASF account passwords were 4-digit PINs. SRL and ASF members’ PINs were set to their birthdates by default, and their access was subject to an automatic lockout in the event of 5 failed login attempts within a 24-hour period. This password policy made the password spray method effective.

Using the compromised accounts, the threat actor attempted to make HTTP requests from the ASF webpage to access the personal data of other SRL members. Due to a misconfiguration error on the ASF webpage (described below), the threat actor was successful in gaining unauthorised access to customer records of approximately 665,495 SRL members (the “**affected data**”) which the threat actor managed to exfiltrate. The affected data were names, email address, phone numbers, countries of residence and SRL membership numbers and tiers of SRL members.

Investigations revealed that the threat actor had managed to gain unauthorised access to the affected data due to a misconfiguration error during MBS’ migration to a new middleware platform that took place between September 2022 and March 2023. This involved the wholesale replication of the Application Programming Interface (“**API**”) onto the new middleware platform, which MBS had opted to carry out manually. The employee in charge of the API replication manually compiled an inventory of APIs and calling application IDs into an inventory list, but inadvertently omitted the external ArtScience Museum calling app ID. As this list was subsequently used to configure token checks in the new middleware platform, MBS’ token verification policy did not apply to the ASF webpage (the “**misconfiguration error**”).

The misconfiguration error resulted in an acute security vulnerability as anyone who accessed the ASF webpage with a valid access token could manipulate the parameters of the membership ID in their HTTP request in order to access other members’ personal data. This vulnerability was exploited by the threat actor to access the affected data.

The PDPC's Decision

Based on the results of its investigations, MBS admitted to a contravention of the Personal Data Protection Act (the “**PDPA**”), in particular, for failing to put in place adequate security arrangements to prevent the misconfiguration error from arising.

Accordingly, the Personal Data Protection Commission (the “**PDPC**”) held that MBS had breached the obligation under Section 24 of the PDPA to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (referred to by the PDPC as the “**Protection Obligation**”). Given the high volume of personal data in MBS’ possession, the PDPC found that MBS was obligated to implement security measures that were commensurate with its higher level of security needs.

In arriving at this decision, the PDPC reiterated that organisations should not solely rely on their employees to perform their duties properly as a security arrangement. Organisations must also implement reasonable arrangements to ensure that any steps required from employees are properly carried out. If higher volumes and/or sensitivity of personal data are involved and if employees’ actions involve a higher susceptibility to human error, the organisation must implement more robust processes. In this regard, the PDPC highlighted the basic practice of automating build and deployment processes to minimise manual steps and hence reduce human errors, which is set out in its Guide to Data Protection Practices for ICT Systems (though it accepted MBS’ explanation that, in this particular instance, the process could not have been automated). The PDPC did not find the ability, expertise and training of the employee who had carried out the API replication to constitute reasonable security arrangements. MBS should not have placed all responsibility on the employee to carry out the replication properly without additional checks to address the risk of human errors (e.g. independent verification or automation of the API replication process). Based on the above facts, the PDPC consequently found MBS to have negligently breached the Protection Obligation.

In addition to this finding, the PDPC highlighted that organisations must implement basic password requirements such as a minimum password length and complexity although it did not find it necessary to make any breach findings in relation to the access control measures employed by MBS.

The PDPC's Preliminary Decision

In the PDPC’s preliminary decision, it required MBS to pay a financial penalty under Section 48J of the PDPA. In determining whether a financial penalty should be meted out as well as its quantum, the following factors were considered:

- a) The breach of the Protection Obligation resulted in the unauthorised access to and disclosure of 665,495 individuals’ personal data. The vulnerability caused by the misconfiguration error existed for at least 6 months prior to the incident, and the affected data was exfiltrated and put up for sale on the dark web.

- b) Otherwise, MBS had implemented adequate and appropriate security arrangements.
- c) MBS took prompt actions after being informed of the incident to mitigate the effects of the incident and to prevent a recurrence.
- d) The investigations were handled under the expedited decision procedure, where MBS admitted to the facts set out in the PDPC's decision and its breach of the Protection Obligation.
- e) The cooperativeness of MBS in investigations.
- f) MBS' annual turnover in Singapore based on its audited accounts. Pursuant to the Personal Data Protection (Amendment) Act 2021 ("**2021 Amendments**"), the maximum financial penalty imposed for contraventions of Parts 3 to 6A of the PDPA by organisations whose annual turnover in Singapore exceeds S\$10 million has increased from S\$1 million to 10% of their annual turnover in Singapore.

Concerning point (f), the PDPC noted that during the Second Reading of the Personal Data Protection (Amendment) Bill, the then-Minister for Communications and Information had explained that the objective of the new financial penalty range is to ensure that the requisite deterrent effect on organisations is achieved, signalling the importance of data protection in the digital economy (being comparable with other legislation such as the Telecommunications Act 1999 and Competition Act 2004). Thus, given the considerable size of MBS' annual turnover in Singapore, the PDPC found that a proportionately higher financial penalty was necessary to serve a deterrent effect. This was in line with its recent decisions which followed the increased maximum financial penalty brought about by the 2021 Amendments. Organisations are thus reminded that going forward, the size of their annual turnover would continue to be a factor in the PDPC's assessment of the amount of financial penalty to be imposed.

For the reasons set out above, the PDPC imposed an initial financial penalty of S\$450,000 on MBS.

Representations made by MBS

Following the preliminary decision, MBS disputed the imposition of a financial penalty and in the alternative, disputed the quantum thereof. In doing so, the following representations were made:

- a) the PDPC erred in determining that MBS negligently breached the Protection Obligation ("**Representation 1**");
- b) the PDPC erred in law by considering MBS' turnover in Singapore when determining the quantum of the financial penalty to be imposed ("**Representation 2**"); and
- c) regardless of whether the PDPC was empowered to take into consideration MBS' turnover, the quantum of the financial penalty ought to be reduced as the preliminary decision did not sufficiently account for relevant mitigating factors ("**Representation 3**").

In Representation 1, MBS argued that its breach of the Protection Obligation was not “negligent” within the meaning of Section 48J(1)(a) of the PDPA. MBS supported this argument based on the legal standard set out in the Competition and Consumer Commission of Singapore’s Guidelines on Directions and Remedies (effective 1 February 2022) and that it had acted reasonably and not negligently since there was no alternative to manually creating the inventory listing and carrying out the API replication, MBS stated that it had implemented various security arrangements to protect the affected data and MBS had assigned the most qualified employee to lead the API replication exercise.

The PDPC disagreed and explained the following (among other matters):

- a) Non-compliance with the Protection Obligation is the result of an organisation failing to implement security measures that it reasonably should have in light of the risks posed to the data. This is assessed objectively on the basis of two considerations: (i) what the reasonably foreseeable risks posed to the personal data are; and (ii) what security measures the organisation should have reasonably implemented to protect the personal data in its possession or under its control from these risks.
- b) If a risk was reasonably foreseeable and an organisation’s security arrangements (or lack thereof) to reduce, mitigate or eliminate that risk fell below the standard expected of a reasonable organisation, such a breach would necessarily be negligent.
- c) Here, a reasonable organisation ought to have foreseen that an omission in assembling the inventory list manually, especially in a new and complex middleware migration, might create a vulnerability with foreseeable consequences of personal data security. In this regard, MBS had in fact also flagged the misconfiguration of API settings as a risk in a threat risk assessment it had carried out before the migration exercise in January 2022. Given the foreseeable risk of human error embedded in the manual process and the risks involved, it was unreasonable for MBS to rely on the employee to carry out the API replication without any meaningful checks on the accuracy of the inventory list. The employee’s expertise and experience alone were insufficient reason for MBS to rely solely on the employee. There was also no indication that MBS’ pre-deployment checks and post-deployment penetration testing on the new platform could have detected an omission in the inventory list and the misconfiguration error.

For these reasons, the PDPC rejected Representation 1 and maintained its finding that MBS breached the Protection Obligation negligently.

In Representation 2, MBS contended that the PDPC erred in law by considering the size of its turnover when assessing the quantum of the financial penalty to be imposed. In summary, MBS took the position that: (i) Section 48J of the PDPA did not empower the PDPC to take into consideration MBS’ annual turnover when determining the amount of the financial penalty to be imposed, and that (ii) the PDPC’s decision on the preliminary financial penalty infringed Article 12(1) of the Constitution of the Republic of Singapore as it subjected MBS to arbitrary discrimination / unequal treatment:

- a) In relation to (i), MBS' main contention was that Section 48J(3) and 48J(6) of the PDPA did not state that PDPC should take into account an organisation's turnover in determining a financial penalty and that the legislative intent of the increased financial penalty was for ensuring penalties were proportionate to the severity of the data breach and not for enhancing the quantum of the financial penalty based on the organisation's turnover.
- b) In relation to (ii), MBS argued that the financial penalty would cause it to be treated differently from other organisations involved in cases which were "equivalent or similar save for having a lower turnover" and this differential treatment was not based on legitimate reasons which bore a sufficient rational relation to the objective of Section 48J of the PDPA.

In relation to Representation 2, the PDPC explained, on various grounds, why an organisation's annual turnover is clearly a relevant factor when quantifying financial penalties (and this was intended by Parliament), and that differentiating between organisations on the basis of annual turnover is legitimate and lawful in relation to Article 12(1) of the Singapore Constitution, applying the 2-step framework under the Court of Appeal's decision in *Syed Suhail bin Syed Zin v Attorney-General* [2021] 1 SLR 809. For these reasons, PDPC rejected Representation 2.

Finally, in relation to Representation 3, the PDPC took into account the matters raised by MBS and accorded greater mitigatory weight to the overall prompt and voluntary remedial measures taken by MBS. Accordingly, PDPC reduced the financial penalty from S\$450,000 to S\$315,000.

Financial Penalty Framework under the amended PDPA

To promote clarity and consistency, the PDPC took the opportunity in this decision to articulate key aspects of its financial penalty framework ("**Penalty Framework**") for determining the quantum of financial penalties under the PDPA as it had been amended in 2021. The PDPC emphasised that this framework is a guide which may be updated as appropriate and it does not limit or restrict the PDPC's powers under the PDPA.

The Penalty Framework is subject to the following guiding principles:

- a) effectively deterring non-compliance with the PDPA, while ensuring proportionality to the seriousness of the non-compliance;
- b) when considering the relative weight to be given to effective deterrence and proportionality, consideration has to be given to the PDPA's overarching balance of the right of individuals to protect their personal data and organisations' need to process personal data for legitimate purposes;
- c) like and consistent treatment in the two-tiered financial penalty regime for organisations with annual turnovers of S\$10 million and below, and organisations with annual turnovers above S\$10 million. Annual turnover size should be accorded more weight for organisations with annual turnovers above S\$10 million. Other relevant factors must be given similar weight in like cases; and

- d) the Penalty Framework must be applied in a fact-sensitive manner.

With these in mind, the Penalty Framework comprises the following steps:

- a) **Preliminary Step:** The PDPC first determines the statutory maximum financial penalty from Section 48J(3) of the PDPA. Thereafter, it applies a percentage rate or quantum cap (not exceeding the maximum financial penalty) based on the nature of the contravention. Intentional contraventions tend to attract a higher percentage rate than negligent contraventions. This results in the maximum financial penalty in a given case.
- b) A five-step methodology then applies:
 1. **Step 1: Identification of level of culpability and harm.** The PDPC considers all relevant factors to determine whether the organisation's level of culpability is "low", "medium" or "high". Some of these factors include, but are not limited to the nature, gravity and duration of non-compliance. Thereafter, the PDPC will determine whether the level of harm is "slight", "moderate" or severe" considering all relevant matters. Such matters include, but are not limited to the type, nature and sensitivity of the affected data, the number of affected individuals and the extent of harm or prejudice caused to individuals.
 2. **Step 2: Calculation of the starting financial penalty.** Based on the levels of culpability and harm determined in Step 1, the PDPC will identify the indicative levels of culpability and harm to determine the starting range and within that range, determine the approximate starting financial penalty to be imposed.
 3. **Step 3: Adjustment for aggravating and mitigating factors.** Thereafter, the PDPC will adjust the starting financial penalty identified in Step 2 for relevant aggravating and mitigating factors.
 4. **Step 4: Consideration of the likely impact of the financial penalty on the organisation's ability to continue usual activities.** The PDPC will determine the likely effect the financial penalty would have on the organisation's financial health. The onus is on the organisation to make representations, supported by evidence, to the PDPC. If it is found that the organisation's ability to carry on its activities would be adversely affected, the PDPC may extend the timeline for payment, allow for its payment to be made in instalments, or reduce the quantum of the financial penalty.
 5. **Step 5: Final adjustments.** As the last step, the PDPC will make final adjustments to the quantum so as to ensure the outcome is both effective and proportionate, ensuring that an appropriate balance is struck between achieving effective deterrence and ensuring proportionality.

Application of the Penalty Framework to this Case

Applied to the present case, the PDPC found that the maximum financial penalty applicable to MBS was 10% of its annual turnover and that it had committed a negligent contravention of the Protection Obligation. Applying Step 1, it was found that MBS' **level of culpability was low** although the **level of harm was**

moderate due to the large number of affected individuals. Thereafter, the PDPC determined the starting range and approximate starting financial penalty within the low-moderate band. Relevant mitigating factors were taken into consideration. In connection with this, the PDPC noted that MBS' first PDPA non-compliance was a neutral factor, although its voluntary notification to affected individuals enabled individuals to take prompt steps to safeguard their interests and thus accorded some additional mitigatory weight. MBS' prompt and voluntary remedial measures were also accorded greater mitigatory weight. Overall, this resulted in a reduced financial penalty of S\$315,000. The PDPC found that this amount would not adversely affect MBS' ability to carry out its usual operations. No further adjustments were made in light of all the relevant facts of the case.

Conclusion

This case underscores the need for organisations to ensure that adequate processes are put in place to ensure that any action required from employees is properly taken. In particular, organisations cannot rely solely on their employees performing their duties properly as a measure to safeguard personal data. Where employees' actions may affect personal data that are more sensitive or greater in volume, and where such actions are more susceptible to human error, organisations should implement more robust processes to check the work of their employees.

In relation to PDPC's financial penalty framework for contraventions of the PDPA, deterring non-compliance with the PDPA has emerged as a significant goal of the PDPC when imposing financial penalties, signalling a more proactive enforcement approach will likely be taken by the PDPC in the future.

While it was noted that the financial penalty issued under this decision by the PDPC is the second highest to-date for a contravention of the PDPA, it is also significant that this case did not concern particularly sensitive personal data. In comparison, the previous highest and second highest penalties were issued in connection with highly sensitive personal data of 159,000 affected individuals (namely certain healthcare data, per *Re Singapore Health Services Pte. Ltd. & Ors.* [2019] SGPDPC 3). This is a strong indication that even higher financial penalties may be expected in the future, particularly for cases that involve personal data of higher sensitivity or greater potential harm to the affected individuals.

The PDPC's elucidation of its Penalty Framework is a welcome development as it provides greater insight into how the regulator approaches financial penalties, which is a common concern for organisations. With such clarification, organisations may be better able to analyse trends in the PDPC's enforcement which should inform their data protection and cybersecurity priorities.

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



Lim Chong Kin

Managing Director,
Corporate & Finance
Head,
Telecommunications,
Media & Technology
Co-Head, Data
Protection, Privacy &
Cybersecurity
Co-Head, Competition
Law & Regulatory
Practice
Drew & Napier LLC

T: +65 6531 4110
E: chongkin.lim
@drewnapier.com



David N. Alfred

Director, Corporate &
Finance
Co-Head, Data
Protection, Privacy &
Cybersecurity Practice
Drew & Napier LLC

T: +65 6531 2342
E: david.alfred
@drewnapier.com



Anastasia Chen

Director, Corporate &
Finance
Deputy Head, Data
Protection, Privacy &
Cybersecurity Practice
Drew & Napier LLC

T: +65 6531 4123
E: anastasia.chen
@drewnapier.com

Private Client & Private Client Disputes Legal Update

Court Upholds Will — Disinherited Wife’s Challenge Fails; Half-Sister Inherits Estate *XAT v XAU and another* [2025] SGHCF 4

Introduction

XAT v XAU and another [2025] SGHCF 4 concerns the validity of a will made by the deceased (the “Will”), who excluded his wife, the appellant, from his Will, and instead left his estate to his half-sister.

The General Division of the High Court (Family Division) upheld the Family Court’s decision, *ie* that the Will was rational on its face, and therefore inclined the Court towards the finding that the deceased had testamentary capacity, and that he knew of and approved of the Will.

Background

The appellant, a Chinese national, had initially come to Singapore under a Long-Term Visit Pass to accompany her daughter, who was studying in the country. In 2011, the appellant became a tenant in the deceased’s flat. The appellant married the deceased in October 2013 and continued living in his flat.

In October 2014, the appellant and the deceased were interviewed by reporters. In the two articles that were published the next day in local Chinese papers, the deceased reportedly claimed that the parties had not consummated their marriage. He also alleged the appellant had asked him to register the marriage with her, which he did so out of sympathy. The appellant also allegedly caused the deceased’s other tenant to leave, refused to pay rental and utility bills, and took “relics” which belonged to the deceased’s mother. As the deceased was unable to tolerate the appellant’s behaviour, he suggested that they annul the marriage, but the appellant refused.

After the articles were published, the appellant started paying rent to the deceased on a monthly basis. The deceased issued the appellant receipts confirming “payment for the water and electricity bills, taxes and other miscellaneous charges”, and that “[the appellant] is responsible for the daily living activities of [the deceased].” The deceased also signed a letter which authorised the appellant to rent out one room, and specified that the appellant shall be responsible for all matters relating to the room rental, pay a monthly sum to the deceased, and continue to be responsible for the deceased’s daily living activities. The deceased took no steps to annul the marriage or divorce the appellant.

In July 2015, the deceased became hospitalised. According to the deceased’s friend, who visited him at the hospital, the deceased allegedly told him that the appellant did not visit him during his hospitalisation, and their marriage was a sham. The deceased then shared that he did not wish to leave his flat to the appellant and instead wished to leave it to his half-sister. He then instructed his friend to prepare his Will, which appointed his nephew as the executor and trustee, and included the following at paragraph 6:

“I DO NOT wish to give any of my property or personal properties to my wife ... as I merely ‘marry’ her (sic) to help her extend her stay as an accompanying person to her child who is studying in Singapore. We are unable (sic) to consummate our marriage.”

The deceased’s friend kept the Will on the deceased’s behalf and only informed the appellant about the Will after the deceased passed away.

The appellant commenced proceedings to invalidate the Will, alleging that the deceased did not have the requisite capacity to sign the Will, that the Will was forged, and/or that he was under undue influence when he signed the Will. The deceased’s nephew was named the first respondent, while the deceased’s half-sister was named the second respondent.

The Family Court found that the deceased was not suffering from mental disability, and that the contents of the Will were rational on its face. The Family Court referred to a medical report dated 20 September 2018 from Tan Tock Seng Hospital, which established that the deceased was able to consent to anesthesia and surgery to amputate his left forefoot. Hence, the deceased was presumed to have testamentary capacity.

At trial and on appeal, the appellant argued that the Will was not executed in ordinary circumstances. The Will was allegedly signed five days after the deceased’s operation to amputate his left forefoot. Accordingly, she argued that the deceased would not have had testamentary capacity at the time, and in any event, the deceased would not have been in the right frame of mind to know or approve of the Will’s contents.

The Court’s Decision

On appeal, the Appellate Court upheld the validity of the Will.

Firstly, the Appellate Court reiterated that the party who propounds or puts forwards a will must prove the testator had testamentary capacity when he signed the will. This includes understanding the nature of the act of making a will and its consequences; knowing the extent of his property of which he is disposing, knowing who his beneficiaries are and being able to appreciate their claims to his property, and being free from an abnormal state of mind that might distort feelings or judgments relevant to making the will.

Testamentary capacity is *prima facie* established when the will is executed in ordinary circumstances, *ie* where the testator was not shown to be suffering from any mental disability. The party challenging the will may rebut this presumption by adducing evidence to prove otherwise. When testamentary capacity is established, a rebuttable presumption that the testator knew and approved of the contents of the will would arise. However, this presumption does not arise if there are circumstances that raise a well-grounded suspicion that the will did not express the mind of the testator.

If the will, upon consideration of its terms and the identities of the beneficiaries, does not appear to be rational, this may indicate that the testator lacked

testamentary capacity and there are surrounding suspicious circumstances. The test is whether the Court is satisfied that the contents of the will truly represent the testator's testamentary intentions.

Here, the Appellate Court agreed that the Will was not executed in "ordinary" circumstances, and the circumstances raised suspicions that the Will did not express the deceased's mind. However, the medical report dated 20 September 2018 did refer to the deceased's medical records of 17 August 2015, the date on which the Will was dated, which showed that he was alert, comfortable, oriented to time, place and person and with stable vital signs. This pointed towards the deceased having testamentary capacity. This was corroborated by the Family Court's finding that the respondents have shown that the deceased had testamentary capacity, with the first respondent, the deceased's friend, and the witnesses and interpreter of the Will having testified as to the lucidity of the deceased. These individuals did not appear to have anything to gain from the Will, given that they are not directly related to the beneficiary of the Will, the second respondent.

Secondly, the Appellate Court did not disturb the Family Court's finding that the Will was rational on its face, the deceased had testamentary capacity, and he knew and approved the Will. The burden would be on the appellant to show that the Will was irrational. She could prove that by showing either (a) that she had no need to marry the deceased to extend her stay or (b) that the marriage was not a sham.

As regards (a), the appellant claimed she could stay until 2018 under her Long-Term Visit Pass. However, she had not shown that she had no need to marry the deceased to extend her stay, given that she could have been looking to stay beyond 2018, and that her daughter was not yet a Singapore Permanent Resident or citizen when the appellant married the deceased.

As for (b), the appellant had not produced objective evidence or sufficient testimony to show that her marriage was not a sham. Her two friends' evidence did not mention how the appellant and the deceased interacted after marriage. Additionally, as the deceased had accompanied the reporters into the flat, the Family Court was entitled to conclude that deceased would not bring someone into his flat without knowing who they were or why they were there. Separately, the Appellate Court found the receipts signed by the deceased to be a neutral factor which could both support the argument that they were for the appellant's benefit; or that there was a contractual relationship between the appellant and the deceased.

The remainder of the appellant's arguments (*ie* that the Will was forged and that the deceased was under undue influence when he executed the Will) also failed as she was unable to provide sufficient evidence supporting the same.

Commentary

a) Establishing testamentary capacity

Firstly, this case illustrates the importance of establishing testamentary capacity. Where a testator's capacity can be challenged, *eg* where they are of old age and / or unwell, it would be prudent to procure a doctor to (a) act

as a witness to the will, or (b) certify that the deceased had testamentary capacity and was in the right frame of mind to approve of the will's contents prior to execution. This would preferably be the testator's regular doctor, who would be well-placed to undertake the assessment, or a psychiatrist if mental infirmities are involved.

Where the testator suffers from mental infirmities, the solicitor preparing the will and / or witnessing the execution should attend to him personally to take instructions, provide him with the draft will and explain the same to him. Furthermore, the solicitor should ask appropriate questions to ascertain the testator's capacity in understanding the contents of the will (eg whether he is making a will for the first time; and if he had made a will previously, whether he knows that he is revoking his existing will), and keep contemporaneous attendance notes in this regard.

b) Exclusion of beneficiaries

Secondly, while testators may attempt to exclude certain family members from their will, pursuant to the Inheritance (Family Provision) Act 1966 ("IFPA"), if the Court, on application by the deceased's dependents, is of the opinion that the disposition of a deceased estate does not make reasonable provision for their maintenance, the Court may order for the same to be made out of the deceased's estate. In practice, however, the provisions in the IFPA are rarely used in Singapore, and parties usually attempt to contest the validity of the will instead. Additionally, the application of the IFPA is narrow in nature, with its purpose limited to the provision of reasonable maintenance and not for the purpose of seeking a share of the testator's estate. The definition of dependents provided for therein is also limited. For example, illegitimate children would not be able to leverage the IFPA provisions in making a claim.

Notably, in determining whether to exercise such powers under the IFPA, the Court will take into account various factors, including the conduct of the dependent in relation to the deceased and the deceased's reasons for the refraining from making certain dispositions or provisions. Therefore, when drafting wills that exclude certain beneficiaries, it may be prudent to explain the reasons for their exclusion in the will itself, for example that sufficient provision had been made during the testator's lifetime, and / or there was a breakdown in the relationship etc. This helps shed light on the testamentary intentions of the testator and justify seemingly "irrational" provisions.

c) Consequences of marriage

If the will was found to be invalid and the deceased had no other will, the appellant wife may have been entitled to make a claim on the basis that he had died intestate. The estate would then have to be distributed pursuant to the Intestate Succession Act. As such, marriages of convenience or sham marriages should not be entered into lightly, since there are consequences on death.

d) Seeking professional legal advice

Lastly, this case serves as a timely reminder for testators to engage qualified solicitors in drafting wills. This avoids problems such as issues of

interpretation stemming from ambiguous wording, challenges to the will's validity, and gaps in coverage which could leave part of the estate to be dealt with through intestacy.

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



Seah Ching Ling

Director, Tax and
Private Clients Services
Drew & Napier LLC

T: +65 6531 4102
E: chingling.seah@
drewnapier.com



Hoon Shu Mei

Director, Private Client
& Family Disputes
Drew & Napier LLC

T: +65 6531 2223
E: shumei.hoon@
drewnapier.com



INDONESIA

MAKARIM & TAIRA S.

Corporate Compliance Legal Update

Indonesia Simplifies Market Entry, Strengthens Compliance — Insights from Head of BKPM Regulation 5/2025

In an effort to attract more foreign investment and improve legal certainty, Indonesia has streamlined its risk-based business licensing system by lowering capital thresholds and introducing automatic approvals, while also tightening post-licensing supervision and enforcement.

The system's overhaul was mandated under Government Regulation No. 28 of 2025 on the Implementation of Risk-Based Business Licensing, issued on 5 June 2025. In line with this, the Minister of Investment and Downstream Industry/Head of the Investment Coordination Board ("BKPM") has issued Regulation No. 5 of 2025 on Guidelines and Procedures for the Implementation of Risk-Based Business Licensing and Investment Facilities Through the Electronically Integrated Business Licensing System (Online Single Submission – "OSS") ("**Regulation 5/2025**" or the "**Regulation**"), which took effect on 2 October 2025.

Regulation 5/2025 revokes and replaces the following BKPM regulations:

- a) BKPM Regulation No. 3 of 2021 on Electronically Integrated Risk-Based Business Licensing.
- b) BKPM Regulation No. 4 of 2021 on Guidelines and Procedures for Risk-Based Business Licensing Services and Investment Facilities.
- c) BKPM Regulation No. 5 of 2021 on Guidelines and Procedures for Risk-Based Business Licensing Supervision.

Regulation 5/2025 is an important step in Indonesia's efforts to modernise and streamline investment procedures. By reducing capital requirements, providing clearer licensing stages, expanding digital supervision, and introducing mechanisms such as the tacit approval (*fiktif positif*) policy and simplified reporting, this regulation is expected to create a more efficient, transparent, and investor-friendly environment.

The Regulation spans 256 pages, or 698 pages including its attachments, and sets out detailed provisions on risk-based business licensing. This advisory highlights fifteen key takeaways from Regulation 5/2025.

Minimum Capital Requirement and Investment Value

a) **Minimum Capital Requirement:**

Regulation 5/2025 reduces the minimum issued and paid-up capital for foreign investment companies from IDR 10 billion to IDR 2.5 billion.

This capital cannot be transferred for 12 months after being deposited into the company's account (12-Month Restriction), unless it is used for legitimate

business purposes such as buying assets, constructing buildings, or funding operations.

b) **Minimum Investment Value:**

Foreign investment companies are classified as large-scale businesses and must invest more than IDR 10 billion per 5-digit Indonesian Standard Business Field Classification (“**KBLI**”) per project location, excluding land and buildings.

Exceptions apply to the following sectors, where the investment threshold is measured differently:

1. Wholesale trade – per 4-digit KBLI.
2. Food and beverage services – per 2-digit KBLI per city/regency.
3. Construction services – per 4-digit KBLI.
4. Manufacturing – for multiple products produced in one production line.

Land and building values may be included in the investment total for certain sectors, such as property, accommodation, agriculture, plantations, livestock, and aquaculture.

For property development and management, the IDR 10 billion investment threshold applies:

1. including land/buildings for integrated projects (entire buildings or housing complexes); or
2. excluding land/buildings for individual property units outside integrated projects.

Basic Requirements: Spatial, Environmental, and Building-Related Approvals

Under the previous regulation, the basic licensing requirements primarily covered spatial conformity, environmental approval, and building approvals. Regulation 5/2025 expands the scope of the implementation of Risk-Based Business Licensing (“**PBBR**”) to include:

- a) Conformity of Spatial Utilisation Activities (KKPR), Conformity of Marine Spatial Utilisation Activities (KKPRL), and/or forest area approval;
- b) Environmental Approval (PL); and
- c) Building Construction Approval (PBG) and Certificate of Feasibility (SLF).

It also introduces a more detailed classification of basic requirements, including for land and marine spatial conformity (KKPR *Darat* and KKPR *Laut*), forest area approvals (including recommendations and technical considerations), environmental approvals, building approvals, and specific requirements for micro, small, and ultra-small businesses.

Issuance of Business License (“PB”), including the *fiktif positif* approach

The *fiktif positif* (tacit approval) mechanism means that if an applicant meets all requirements and the government fails to respond within the Service Level Agreement (SLA) period, the license will be automatically approved.

The main objective of the *fiktif positif* policy is to accelerate the licensing process and ensure legal certainty for investors. The policy will be implemented gradually for all risk-based licensing processes under 5/2025, starting with sectors such as agriculture, energy and mineral resources, marine affairs and fisheries, manpower, industry, and tourism.

Issuance of Supporting Business Licensing (“PB UMKU”)

PB UMKU can be applied for through the OSS System, either before or during a company’s operational or commercial phase.

PB UMKU covers licenses for: (i) product distribution; (ii) operational feasibility; (iii) product or service standardisation; and (iv) other business facilitation needs.

Certain high-risk business activities may obtain accelerated PB UMKU if they are:

- a) located in Special Economic Zones, Free Trade Zones, or Industrial Estates; or
- b) part of a National Strategic Project.

Supervision Measures**a) Coordinated Supervision and Data Integration:**

Regulation 5/2025 envisions a coordinated supervision system, where supervision results from one authority are recognised across others. To enable this, the OSS System is expected to enhance its data integration capabilities, linking with national registries, regional licensing databases, as well as sectoral information systems. In practice, this could mean less duplication but more accountability, as supervision results will be centrally recorded and accessible across institutions.

b) Two-tier Supervision: Regular and Incidental:

Regular supervision refers to periodic and planned monitoring activity conducted according to a predefined schedule. Incidental supervision, on the other hand, refers to trigger-based and unplanned monitoring conducted in response to, among other things, public complaints (**either through complaint channels or social media**), indications of non-compliance, as well as urgent and unforeseen events. Therefore, it is conducted through incidental site inspections with no prior notification to the targeted businesses.

c) **Business Actor Profiling:**

Business actors will have a profile that aggregates data from licensing records, supervision reports (either regular or incidental), and other administrative databases. This profile allows authorities to categorise businesses according to their compliance behavior and operational characteristics.

The OSS System automatically processes Investment Activity Report (*Laporan Kegiatan Penanaman Modal – “LKPM”*) verification data and regular site inspection results to assign each business actor a compliance score (either very good, good, fair, or poor), which then determines the compliance profile of the business. The follow-up actions prescribed include:

1. coaching or assistance, intended to maintain a high level of compliance and provide continuous support, including technical guidance;
2. administrative sanctions for businesses with a compliance level of ‘fair’ or ‘poor’; and
3. site inspections, either through regular or incidental supervision.

Minimum Investment for Public Electric Vehicle Charging Stations (SPKLU)

Regulation 5/2025 introduces a new minimum investment requirement of more than IDR 10 billion, excluding land and buildings, for public electric vehicle charging stations (SPKLU) **within one province**.

Representative Offices – KPPA and KP3A

Regulation 5/2025 updates the framework for Representative Offices (“RO”), covering the following types:

- a) Representative Office of a Foreign Company (*Kantor Perwakilan Perusahaan Asing – KPPA*);
- b) Representative Office of a Foreign Trading Company (*Kantor Perwakilan Perusahaan Perdagangan Asing – KP3A*);
- c) KP3A in Electronic Commerce (*Bidang Perdagangan Melalui Sistem Elektronik – KP3A PMSE*);
- d) Representative Office of a Foreign Construction Services Business Entity (*Kantor Perwakilan Badan Usaha Jasa Konstruksi Asing – BUJKA RO*); and
- e) Representative Office of Foreign Electricity Support Services (*Kantor Perwakilan Jasa Penunjang Tenaga Listrik Asing – KPJPTLA*).

All ROs must now obtain a Business Identification Number (“NIB”), which was not mandatory under the previous regime. The NIB is valid for three years and can be renewed.

In addition, ROs must now submit Investment Activity Reports (LKPM) through the OSS System every six months, except for BUJKA Construction ROs and Foreign Electricity Support ROs, which are required to report annually.

Sanctions

Administrative sanctions for business actors who violate basic requirements, business licensing (PB), or supporting business licensing (PB UMKU) now include **administrative fines** and **administrative coercive measures**, applied in a more systematic and tiered manner to provide a restorative mechanism for violators.

The administrative sanctions consist of:

- a) Written warnings (including (i) first, second and third warnings, and (ii) first and final warning);
- b) Temporary suspension of business activities;
- c) Administrative fines;
- d) Administrative coercive measures;
- e) Revocation of basic requirements, PB and/or PB UMKU.

Highlights of the more detailed administrative sanctions under the new regulations include:

- a) **Temporary suspension:** now explicitly includes situations where a business actor is: (i) prohibited from conducting business activities; and/or (ii) **restricted from conducting corporate actions in the OSS System.**
- b) **Administrative fines:** business actors who fail to pay an imposed fine may face administrative coercive measures or revocation of risk-based business licensing (PBBR).
- c) **Administrative coercive** measures may include:
 - 1. temporary suspension of public services;
 - 2. seizure of goods or equipment that may cause or contribute to a violation;
 - 3. withdrawal of products from circulation;
 - 4. prohibition from operating;
 - 5. closure of premises;
 - 6. demolition of buildings;
 - 7. other actions intended to stop violations that cause damage; and/or

8. other actions in accordance with the provisions of laws and regulations.

Steps in Engaging and Performing Business Activities

The previous regulations only addressed the subsystem of business licensing services without providing a clear breakdown of the stages of business activities. Regulation 5/2025 now establishes a structured framework that divides business operations into two distinct stages:

- a) Starting a business (*memulai usaha*); and
- b) Operating a business (*menjalankan usaha*).

Starting a business stage consists of three sub-stages:

- a) Fulfilment of business legality, such as Minister of Law decree on the legalisation of a company's legal entity status;
- b) Fulfilment of basic requirements, namely KKPR (for land or marine locations), 9 Steps in Engaging and Performing Business Activities and PL (for activities not requiring an Environmental Impact Analysis (“**AMDAL**”) or Environmental Management Effort-Environmental Monitoring Effort (“**UKL-UPL**”)); and
- c) Obtaining or submitting PB/PB-UMKU, where renewal no longer requires re-submission of basic requirements as long as they remain valid.

Once these steps are completed, businesses proceed to the operating stage, which is divided into:

- a) Preparation sub-stage (land acquisition, environmental approvals for AMDAL or UKL-UPL projects, building construction, equipment procurement, human resource preparation, trial production, and business standard compliance); and
- b) Operational/commercial sub-stage (production, logistics, distribution, marketing, and the requirement to obtain SLF prior to occupying any building).

Investment Activity Report (LKPM)

The underlying principle for supervision remains unchanged: all investment activities in Indonesia must be monitored through LKPM submission. Large-scale enterprises, including foreign investment companies, are still required to submit LKPMs quarterly, but the deadline has been extended to the 15th day after the end of each quarter (it had previously been the 10th day).

In terms of business stages, the regulation distinguishes between:

- a) LKPM for the Preparation Stage, for business actors that have not yet commenced operations and/or commercial transactions; and

- b) LKPM for the Operational and/or Commercial Stage, for business actors that are ready to or already operating or conducting commercial transactions.

Both reports generally contain information on investment realisation, employment data, revenue, fulfillment of business obligations, and operational challenges encountered.

Outward LKPM

Indonesian companies investing abroad must now file quarterly LKPM reports (every three months) through the OSS System. The reporting obligations follow the same timelines and principles as those for domestic investment LKPM.

We understand this requirement is part of the government's effort to supervise anti-money laundering practices. Outward LKPM is also expected to form part of the compliance checklist in legal due diligence processes.

Merger, Spin-off, and Dissolution

Corporate restructuring actions such as merger (*penggabungan*), consolidation (*peleburan*), spin-off (*pemisahan kegiatan usaha*), and dissolution (*pembubaran*) are now explicitly accommodated under Regulation 5/2025.

Any deed effecting such actions must be validated in coordination with the Ministry of Law, and the OSS System must be updated with the new licensing data for the surviving or new entity. The NIBs and business licenses of merged, dissolved, or otherwise terminated entities will be automatically cancelled once the deed is accepted and validated in the OSS System.

For spin-offs, business activities, assets, and liabilities may be transferred partially or fully to either affiliated or non-affiliated entities. Both the transferring and receiving entities must update the OSS System accordingly, including registering lines of business and applying for any required licenses. The OSS validation ensures that the newly spun-off entity is properly licensed according to its business activities under the updated structure.

This new update, particularly on spin-offs, provides greater legal certainty. It comes as state oil and gas company Pertamina prepares to spin off its non-core businesses as part of a restructuring strategy, which includes the potential merger of its aviation subsidiary, Pelita Air, with state-owned airline Garuda Indonesia. Another signal in the market is that the Financial Services Authority (OJK) recently disclosed that several major Islamic banks are planning spin-offs or restructurings in the near future.

Ease of Direct Construction in Industrial Estates (*Kemudahan Langsung Konstruksi di Kawasan Industri – KLIK*)

Businesses engaging in high- or medium-high-risk activities in Industrial Estates may benefit from direct construction facilitation, which allows construction to

begin before all permits are finalised. This is part of the government's investment simplification policy.

Through the OSS System, eligible businesses automatically receive an NIB and supporting documents (an unverified Standard Certificate or a provisional license) authorising pre-operational activities such as construction and trial production.

Before commencing full operations, a business must fulfill all licensing requirements, standards, and applicable payments. If these are not met, the provisional license will become invalid. The OSS System will automatically issue reminders to the business of any pending requirements.

Public Participation and Reports

Public participation is now formally recognised. The public and business actors may participate in supervising business activities by submitting complaints either directly or electronically via the OSS System. Each complaint must be substantiated and will trigger verification, clarification, and, where necessary, enforcement actions or sanctions.

Administrative Branch Office

Regulation 5/2025 introduces the requirement to register administrative branch offices through the OSS System. These branches function solely for administrative purposes and are located separately from the head office or main business site. They are not allowed to conduct commercial activities. If a company has multiple administrative branches, it must submit data for each location.

Regulation 5/2025 required the OSS Agency to adjust the OSS System to comply with the new provisions by 5 October 2025. Its transitional provisions state that verified and approved basic requirements, business licensing (PB), and supporting business licensing (PB UMKU) issued through the risk-based OSS System before Regulation 5/2025 took effect remain valid in accordance with applicable laws and regulations.

Furthermore, applications for basic requirements, PB, PB UMKU, or investment facilities that were still being processed when the OSS System under Regulation 5/2025 became operational (i.e., by 5 October 2025) continue to be processed under BKPM Regulation No. 4 of 2024. Applications that remained unprocessed after that date are returned to the business actors, who must then submit new applications in accordance with Regulation 5/2025.

As Indonesia continues to streamline its investment environment, understanding the impact of Regulation 5/2025 will be key for businesses looking to stay compliant and competitive in this evolving market. Contact us to learn more about how these changes may affect your business in Indonesia.

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



Stephanie Kandou

Partner,
Makarim & Taira S.

T: +6221 5080 8300,
2521272

E: stephanie.kandou
@makarim.com



Maharanny P. Hadrianto

Senior Associate,
Makarim & Taira S.

E: maharanny.hadrianto
@makarim.com



Rininta Shafira

Senior Associate,
Makarim & Taira S.

E: rininta.shafira
@makarim.com



Ivan Juan Alfreda

Associate,
Makarim & Taira S.

E: ivan.alfreda
@makarim.com



**Kaila Arinta
Nazneen Z**

Associate,
Makarim & Taira S.

E: kaila.nazneen
@makarim.com



**Flaviana Meydi
Herditha**

Associate,
Makarim & Taira S.

E: flaviana.herditha
@makarim.com



**Alya Azalia Permata
Sari**

Associate,
Makarim & Taira S.

E: alya.sari
@makarim.com



MALAYSIA

SHEARN DELAMORE & CO.

Employment & Industrial Relations Legal Update

Industrial Court Upholds Dismissal over Verbal Sexual Harassment

Introduction

The Industrial Court in *Camillius Casimir v Genting Malaysia Berhad* (Award No. 1615 of 2025) upheld the dismissal of a security guard who was dismissed for verbally sexually harassing a female employee.

Although the case revolved around a single formal charge of misconduct, the Court emphasised the seriousness of the behaviour, especially given the security guard's role and responsibility within the organisation.

Facts of the case

The incident at the centre of the case involved the security guard ("**the Claimant**") asking a female employee ("**the said female employee**"): "*Amoi, makan hot dog ya?*" ("Young girl, eating hot dog, right?") at the breakfast area.

The Claimant did not dispute that he had uttered the impugned words towards the said female employee, alleging that he was innocently inquiring as to whether she had taken the grilled sausage, aka, hotdog, and that there was nothing sinister in his question or remark to the said female employee.

Genting Malaysia Berhad's ("**the Company**") position was that the Claimant's impugned words to the said female employee contained sexual overtones, in that the word "*hotdog*" in the context of the Claimant's conversation with the said female employee referred to the male genitalia.

During the investigation interview, the said female employee testified that she felt uncomfortable and disgusted with the Claimant's remarks, especially where it was coupled with the Claimant's lewd facial expression.

Whilst the Claimant contended that the impugned words and the circumstance in which it was uttered (it was breakfast time and grilled sausage was indeed served on that day) were innocuous and innocent, the Court found that the Claimant's answers during the investigation interview painted a completely different perspective and context in which he made the remarks to the said female employee.

The Claimant had informed the Company's investigators: "*Saya cuba menegurnya kerana minat melihat dia*" ("I tried to talk to her because I was interested in her").

Decision of the Industrial Court

The Industrial Court reaffirmed that the test in sexual harassment cases is whether the sexual conduct complained of is unsolicited or unreciprocated by the victim/recipient. Further, although the charge against the Claimant

contained only one allegation — the “*hotdog*” remark – the Court took into consideration evidence of the Claimant’s pattern of conduct towards other female staff in the Company whereby he had been preying on some of these female staff with making remarks containing sexual overtones or innuendo.

The Court ruled that the reason operating in the mind of the Company when they dismissed the Claimant from employment was that he had been guilty of a serious act of misconduct, that is, sexual harassment. As such, any evidence that further fortifies the Claimant’s alleged act of sexual harassment towards other female staff in the Company would be admissible.

A key factor in the Court’s ruling was the Claimant’s position. As a security guard, the Claimant was entrusted with the responsibility of ensuring a safe working environment for the Company’s employees, besides ensuring the safety of the premises for the customers of the Company. By engaging in conduct that created discomfort and undermined the sense of safety in some of the female employees, the Claimant had destroyed the trust and confidence reposed in him by the Company.

The Industrial Court expressly recognised that verbal innuendo — even when phrased indirectly or framed as casual conversation — can amount to sexual harassment. By affirming that such behaviour constitutes serious misconduct, the decision aligns industrial jurisprudence with modern expectations of workplace safety — where protecting employees from sexual harassment is an essential component of a safe and respectful working environment. The Industrial Court’s decision further reaffirms that employers have the right to act decisively to preserve a safe workplace.

Copyright © 2025 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.

CONTACTS



Jamie Goh

Partner, Employment &
Industrial Relations
Shearn Delamore & Co.

T: +603 2027 2731

E: jamie.goh
@shearndelamore.com



Peter H. Santiago

Associate, Employment
& Administrative Law
Shearn Delamore & Co.

T: +603 2027 2778

E: peter.santiago
@shearndelamore.com



CAMBODIA

TILLEKE & GIBBINS

Employment Legal Update

Not So Fast: Scaling Back DEI May Violate Local Laws in Southeast Asia

Multiplicity, evenhandedness, and belonging... Variety, balance, and a warm welcome... US companies are searching for synonyms; the thesauruses of their in-house counsel are now dog-eared and well thumbed. In the wake of US President Donald Trump's executive orders to eliminate diversity, equity, and inclusion ("DEI") programmes within the federal government and to direct federal agencies to act against DEI policies in the private sector, some American companies have scrambled to change their language. With President Trump's direction to prosecute discrimination alleged to be under the guise of DEI, using the term "DEI" on a company website risks painting a big red target on those companies.

While some have opted to adjust the descriptions of their programs aimed at improving the status of marginalised groups, others are scrapping their DEI programs entirely. However, US-invested companies should be cautious in eliminating their DEI programmes globally, as some elements of these programs are obligations under local laws. In this article, we note some key points for American companies to consider in respect to their subsidiaries based in Vietnam, Thailand, and Cambodia.

Background

President Trump [issued](#) an executive order on January 21, 2025, titled "Ending Illegal Discrimination and Restoring Merit-Based Opportunity." Among other things, this executive order instructs the attorney general to cooperate with the heads of federal agencies to identify private-sector companies with discriminatory DEI programs. This executive order is premised on the idea that actions favoring members of marginalised groups over majority or dominant groups constitute illegal discriminatory action. An example of this would be hiring quotas for women or visible minorities, which this worldview alleges has resulted in white male candidates being turned down in favor of female or black candidates.

Public companies and large nonprofit organisations identified as engaging in illegal discriminatory conduct through their DEI programs may be subject to civil compliance investigations. Other companies in the private sector could also face public and private actions arising from allegations of breaching nondiscrimination statutes and orders. Thus, any actions taking into consideration race, sex, sexual orientation, disability, or an individual's membership in a marginalised group in making employment decisions may be considered illegal discrimination and be subject to legal action. This risk is what has led many US companies to recharacterise their DEI programs or eliminate them altogether.

Considerations for Vietnam

Positive discrimination for the protection of vulnerable groups

Vietnam defines discrimination in the context of employment differently than the US. Vietnam's Labour Code states, "Discrimination, exclusion, or preference arising from specific job requirements or actions to sustain and protect

employment for vulnerable workers will not be considered discrimination.” Accordingly, Vietnamese labour law stipulates some benefits and protections aimed at sustaining and protecting employment for vulnerable groups, particularly women in the context of maternity or raising a young child.

The Labour Code provides various accommodations to female employees that could be considered discrimination under the Trump administration’s current view of DEI programs, since they provide benefits to female employees that are not offered to male ones. Pregnant employees engaged in labour-intensive, hazardous, or toxic work may request a transfer to a safer or less demanding role or may opt for a one-hour reduction in their daily working time without a reduction in pay. These adjustments must be made without affecting the employee’s salary, benefits, or other lawful entitlements. Additionally, from the seventh month of pregnancy—or the sixth month in remote, upland, border, or island regions—employers are barred from assigning night shifts, overtime, or long-distance travel. Additional protections apply to nursing mothers. They cannot be required to work night shifts or overtime, or travel for business without their consent. Moreover, they are entitled to a fully paid 60-minute break during each working day, which is considered part of their regular working hours.

Female employees also enjoy additional protection from termination of employment not provided to their male counterparts. Female employees are protected from unilateral termination or dismissal while pregnant or on maternity leave. Both male and female employees enjoy protection from dismissal while raising a child under 12 months old.

Vietnamese labour law also focuses on protecting women from sexual harassment, which may be a key aspect of corporate DEI programs. Employers are required to include detailed regulations in their internal labour regulations (the official working rules of the employer registered with the labour authority) regarding how sexual harassment complaints will be investigated and addressed. Additionally, employers are required to ensure their employees are aware of and understand these regulations.

Consequences of eliminating protective measures and benefits that do not apply equally to all employees

If US-invested companies in Vietnam adopt a view of discrimination that insists upon the completely equal treatment of all employees, and they fail to implement the additional benefits and protections afforded to female employees under the Labour Code, they may face wrongful termination lawsuits and administrative fines.

If a Vietnamese subsidiary of a US company terminates or dismisses a female employee while she is entitled to protected status under the law and she brings a wrongful termination lawsuit and wins, she would be entitled to remedies that could include mandatory reinstatement and various levels of compensation depending on the specific circumstances.

For each act of failing to provide the additional rights and entitlements to female employees mentioned above, organisations may face administrative fines ranging from VND 20 million to 40 million (approx. USD 765–1,530).

If sexual harassment occurred in the workplace, the employer could face an administrative fine ranging from VND 30 million to 60 million (approx. USD 1,150–

2,300) and could additionally face civil liability for the acts of its employee if they were performed in the course of their performance of job duties.

Considerations for Thailand

Thailand's Labour Protection Act ("**LPA**") provides foundational protections for employees, including provisions that support gender equality and prohibit workplace harassment.

The LPA explicitly prohibits sexual harassment in the workplace. Employers, supervisors, and inspectors are forbidden from engaging in sexual harassment, making sexual threats, or otherwise disturbing employees in a sexual manner. Violations can result in fines of up to THB 20,000 (approx. USD 615), in addition to civil claims and other remedies. Thus, if issues such as sexual harassment are neglected as part of abandoning DEI, employers may face consequences.

Special protections for female and pregnant employees

The LPA outlines specific protections for female employees that are not afforded to male employees—particularly in relation to hazardous work environments. Employers are prohibited from assigning women to the following tasks:

- a) Mining or construction work underground, underwater, in a cave, or in a tunnel or mountain shaft, except where the conditions of work are deemed to be not harmful to the health or body of the female employee.
- b) Work on scaffolding 10 meters high or above.
- c) Handling or transporting explosive or flammable materials, except where the conditions of work are deemed not harmful to the health or body of the female employee.
- d) Other work as prescribed by ministerial regulations.

Additionally, if a female employee is required to work between midnight and 6:00 a.m. and a labour inspector deems the work to be hazardous, the employer must adjust her working hours accordingly.

Pregnant employees receive further protections, as employers cannot require pregnant workers to:

- a) Operate vibrating machinery or engines;
- b) Drive or travel on vehicles;
- c) Lift or carry loads exceeding 15 kilograms;
- d) Work on boats; or
- e) Perform other tasks that are restricted by ministerial regulations.

Pregnant employees are also protected from working overtime, on holidays, or between 10:00 p.m. and 6:00 a.m., unless they hold executive, academic, clerical, or financial roles and consent to such work without health risks. Pregnant

employees may also present medical certification to request temporary reassignment to more suitable duties before or after childbirth, and employers are obligated to consider such requests.

Employment of persons with disabilities

Under the Empowerment of Persons with Disabilities Act, employers with 100 or more employees are required to promote inclusive hiring practices by employing persons with disabilities at a ratio of at least one person with a disability for every 100 employees.

If an employer does not meet this employment ratio, they are required to make an annual contribution to the Fund for the Empowerment of Persons with Disabilities, which is used to support rehabilitation, education, occupational training, and welfare services for persons with disabilities. The contribution amount is calculated based on the lowest daily minimum wage from the previous year, multiplied by 365 days and by the number of persons with disabilities who would otherwise have been employed under the quota.

If an employer does not hire persons with disabilities and does not wish to contribute to the fund, alternative compliance options may be available through various types of special arrangements, accommodations, or other forms of assistance to persons with disabilities or their caregivers.

Consequences of eliminating protective measures and benefits that do not equally apply to all employees

In respect to penalties, for failing to provide the additional rights and entitlements to female and pregnant employees mentioned above, employers may be subject to imprisonment for up to six months, a fine of up to THB 100,000 (approximately USD 3,100), or both.

Employers who are required to contribute to the Fund for the Empowerment of Persons with Disabilities but fail to do so, delay payment, or remit an insufficient amount are subject to interest charges on the outstanding balance owed to the fund.

Considerations for Cambodia

Cambodia's laws both broadly protect minority groups from discrimination in employment decisions and set out more specific protections for female employees, disabled employees, and employees with HIV. These additional protective measures could be considered discriminatory under the Trump administration's current perspective on DEI programs.

Special protections for female employees

Women, particularly while pregnant, receive additional protections and benefits under Cambodia's Labour Law. Women are exempt from the provision that allows employers to suspend weekly time off for necessary employees in the case of an emergency. Companies that employ women "must watch over their good behaviour and maintain their decency before the public," which includes a prohibition on sexual harassment.

Pregnant women are entitled to maternity leave of 90 days, a portion of which is paid if they have worked for at least one year for the employer. Employers cannot lay off female workers during their maternity leave or at a time when the end of the notice period would fall during their maternity leave. Women are expected to do only light work during the two months following their maternity leave. For one year after giving birth, women are entitled to use one work hour per day to breastfeed their children while receiving their full salaries. Companies with at least 100 female employees must set up a nursing room and day-care center at the workplace or nearby. Additionally, the Ministry of Labour and Vocational Training issued Instruction No. 015/25 to prohibit discrimination against female employees and prevent employers from suspending the employment contracts of pregnant employees within nine months of their return from maternity leave, with limited exceptions.

Special protections for disabled employees

Cambodia has instituted a recruitment quota for disabled employees. Companies with at least 100 employees must employ disabled workers at a minimum rate of 1% of their total number of employees. Companies with at least 100 employees that surpass the quota and companies with under 100 employees that hire disabled workers despite not being subject to a quota will receive incentives. The regulation establishing this quota also requires employers to make adequate adjustments to the working conditions of disabled employees.

In addition, the Labour Law states that employees who suffer from chronic illness, insanity, or permanent disability are released from the obligation to notify their employer before quitting.

Special Protections for Employees with HIV

Cambodian laws also establish protections for employees with HIV by prohibiting discrimination against employees with HIV and establishing that HIV is not a cause for termination. Furthermore, companies with at least eight employees must establish an HIV/AIDS working group or committee to support employees who have HIV.

Consequences of eliminating protective measures and benefits that do not equally apply to all employees

Infractions of these protective measures for employees in Cambodia are punishable by fines.

For instance, companies that fail to provide female employees with maternity leave as mandated by law, lay off employees during maternity leave, require employees to perform more than light work in the two months following maternity leave, or fail to provide nursing accommodations may face administrative fines of KHR 3,360,000 (USD 840) per incident. Companies that neglect their obligation to set up a nursery are subject to a KHR 1,680,000 (USD 420) fine.

Companies that fail to meet the hiring quota for disabled workers must make a recruitment plan to meet the quota within three years and make a contribution to the Disability Foundation equivalent to 40% of the monthly salary of the lowest-paid employee. If they fail to meet the quota and do not pay the contribution, they will face a fine ranging from KHR 100,000 (USD 25) to KHR 1 million (USD 250).

The Department of Occupational Health of the General Directorate of Labour and Vocational Training has the authority to discipline employers who do not comply with the regulatory protections for employees with HIV, such as failing to set up an HIV/AIDS working group or committee. Discipline comes in the form of providing advice for minor infractions and setting deadlines for compliance for larger infractions.

Conclusion

US-invested subsidiaries in Vietnam, Thailand, and Cambodia must carefully consider their local legal obligations if they contemplate rolling back their global DEI programs. Removing or drastically altering existing DEI programs could result in serious legal violations in Southeast Asia, resulting in subsidiaries facing administrative fines, wrongful termination lawsuits, and loss of reputation. Eliminating DEI trainings, in particular anti-sexual harassment trainings, could similarly expose employers to significant liability.

In Vietnam, Thailand, and Cambodia, actions to accommodate or benefit marginalised groups are not considered discriminatory—in contrast with the view put forward by the Trump administration. Companies should review and tailor their DEI programs to ensure they meet their local legal obligations, avoiding potential lawsuits and liability.

CONTACTS



Sarah Galeski

Counsel
Tilleke & Gibbins

T: +84 28 628 45671
E: sarah.g@tilleke.com



Pimvimol (June) Vipamaneerut

Partner
Tilleke & Gibbins

T: +66 2056 5588
E: june.v@tilleke.com



Jay Cohen

Partner and Director,
Cambodia
Tilleke & Gibbins

T: +855 23 964 210
E: jay.c@tilleke.com



Nu Thi To Nguyen

Senior Associate
Tilleke & Gibbins

T: +84 24 3772 5545
E: nu.n@tilleke.com



Dusita Khanijou

Consultant
Tilleke & Gibbins

T: +66 2056 5535
E: dusita.k@tilleke.com



LAOS

TILLEKE & GIBBINS

Laos Introduces Online Arrival Registration System

On August 15, 2025, Laos' Immigration Police Department introduced a pilot online arrival registration system for foreign passport holders entering the country. Under the new system, visitors to Laos will be able to register their arrival online up to three days in advance and will be exempt from filling out paper forms at the border.

Starting September 1, 2025, online registrations will be accepted at four major international border checkpoints: Wattay International Airport in Vientiane, Luang Prabang International Airport, Pakse International Airport in Champasak Province, and the First Lao-Thai Friendship Bridge linking Vientiane and Nong Khai Province in Thailand.

Foreign passport holders arriving in Laos from this date onward will be able to complete the online registration via the official website of the Department of Immigration: <http://www.immigration.gov.la/>. Upon successful registration, travellers will receive a QR code valid for three days, which must be presented to border authorities upon arrival to verify the registration.

During the pilot phase, which is expected to run until early 2026, travellers who have not registered online will still have the option to complete a paper form at the checkpoint. After the pilot phase, the online registration system will become mandatory nationwide, and paper forms will no longer be accepted.

This initiative marks a significant step toward modernising Laos' immigration procedures. Transitioning from traditional paper-based entry forms to a streamlined digital system will greatly enhance efficiency at border checkpoints. The submission of traveller information ahead of arrival is expected to drastically reduce processing times and alleviate congestion at arrival counters, especially during peak travel periods.

CONTACTS



Prisna Sungwanna

Partner and Director,
Laos
Tilleke & Gibbins

T: +66 2056 5656

E: prisna.s@tilleke.com



Naiyane Xaechao

Associate
Tilleke & Gibbins

T: +856 21 262 355

E: naiyane.x@tilleke.com



MYANMAR

TILLEKE & GIBBINS

Fintech Technology Legal Update

Myanmar Affirms Cryptocurrency Controls

A recent warning from the Central Bank of Myanmar (“**CBM**”) against cryptocurrency use upholds the country’s ongoing strategy of enforcing strict prohibitions on unauthorised cryptocurrency activities while also promoting the controlled development of a central bank digital currency (“**CBDC**”).

The CBM’s warning, issued November 16, 2025, reminded the public of announcements in May 2019 and a notification in May 2020 confirming that all online and offline cryptocurrency transactions are strictly prohibited. The CBM also clarified that no financial institution in Myanmar is authorised to deal with digital currencies. The warning highlighted global risks, such as money laundering, scams, tax evasion, hacking, and severe financial losses caused by price volatility and insufficient regulation. The CBM urged the public to use only legitimate banking channels and avoid illegal cryptocurrency activities.

The warning comes five months after the CBM issued a notification announcing the formation of the Central Committee for the Issuance of a Central Bank Digital Currency. This committee includes senior CBM officials, representatives from relevant ministries and the banking sector, and technology experts. Its main role is to research CBDC models, test secure digital payment systems, and ensure that any future implementation aligns with Myanmar’s monetary policy and financial stability objectives.

Taken together, these two actions illustrate the CBM’s continued pursuit of its dual strategy to promote innovation through CBDC development while prohibiting cryptocurrency use. Businesses should note that while CBDC pilot programs may appear in the future, cryptocurrencies remain off-limits.

CONTACTS



**Khin Pearl Yuki
Aung**

Consultant
Tilleke & Gibbins

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



**Yuwadee Thean-
ngarm**

Partner and Director,
Myanmar
Tilleke & Gibbins

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



Aye Thuzar Hlaing

Senior Associate
Tilleke & Gibbins

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

Technology Legal Update

Myanmar Cybersecurity Law Takes Effect

On July 30, 2025, Myanmar's Cybersecurity Law No. 1/2025 came into effect with the State Administration Council's issuance of Notification 113/2025. The law, which was enacted on January 1, 2025, aims to regulate various aspects of digital security and online activities.

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

- a) **Extraterritorial penalties.** The law contains an important provision that authorises 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 organisation, the minimum fine will be MMK 10 million, and the proceeds will be confiscated.
- d) **Government oversight.** The ministry designated by the government is authorised 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 organisation 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. Non-compliance 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 unauthorised 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 authorisation 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 organisation, 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.

Nonetheless, given that services such as VPNs are very widely used, it remains to be seen how these new far-reaching regulations will actually be enforced.

This article was prepared with the assistance of Tilleke & Gibbins intern Ian Michael Yam.

CONTACT



New Oo

Senior Associate
Tilleke & Gibbins

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



THAILAND

TILLEKE & GIBBINS

Employment Legal Update

Thailand Expands Family Leave Rights and Strengthens Worker Protections

Thailand has amended the Labour Protection Act to significantly expand family leave benefits and strengthen employment protections, effective December 7, 2025. The Labour Protection Act (No. 9) B.E. 2568 (2025), published in the *Government Gazette* on November 7, 2025, provides enhanced maternity and paternity benefits, introduces new childcare leave provisions, and extends labour protections to certain public sector contractors.

Key changes introduced by the amendments are detailed below.

Extended Maternity Leave

Female employees are now entitled to up to 120 days of maternity leave per pregnancy, increased from 98 days. Employers must pay full wages for 60 days, increased from the current 45 days.

New Childcare Leave for Health Complications

Female employees who have taken maternity leave are entitled to an additional 15 days of leave to care for newborns with health complications, disabilities, or conditions that could lead to future medical risks. This leave requires a medical certificate and is compensated at 50% of the employee's regular wage.

New Spousal Childbirth Support Leave

Employees whose lawful spouse has given birth are now entitled to 15 days of paid leave to support their spouse or partner during childbirth. This new leave allowance may be taken before or within 90 days after childbirth, with employers required to pay full wages for all 15 days.

Protection for Public Sector Contractors

The law extends protection to individuals engaged under service contracts with government agencies, including central, regional, and local administrations, state enterprises, and public organisations. When such workers are supervised or controlled in a manner similar to employees, the contracting government agencies must provide them with rights and benefits equivalent to those under the Labour Protection Act, including remuneration, weekly holidays, public holidays, annual leave, sick leave, regulated working hours, and rest periods.

New Annual Reporting Requirement

All employers with 10 or more employees must now submit an annual report on employment and working conditions to the Department of Labour Protection and

Welfare by January of each year. Prior to the amendment, a submission was only required if a labour inspector issued a written request to the employer.

Compliance Recommendations

To ensure compliance before the December 7, 2025, effective date, employers should have:

- a) Reviewed and updated company work rules and internal policies to reflect the extended maternity leave, new paternity leave, and additional childcare leave entitlements; and
- b) Communicated the new rights to employees and HR personnel to ensure clear understanding and consistent implementation.

CONTACTS



**Pimvimol (June)
Vipamaneerut**

Partner
Tilleke & Gibbins

T: +66 2056 5588
E: june.v@tilleke.com



Dusita Khanijou

Consultant
Tilleke & Gibbins

T: +66 2056 5535
E: dusita.k@tilleke.com



**Kantima
Sakruengngam**

Associate
Tilleke & Gibbins

T: +66 2056 5702
E: kantima.s@tilleke.com

Competition and Trade Legal Update

Thailand to Remove Import Duty Exemption for Low-Value Goods

Thailand's Customs Department removed the longstanding *de minimis* exemption, which had waived import duties on goods valued at THB 1,500 or less, effective January 1, 2026. Under the new regime, all imported goods with a declared cost, insurance, and freight ("CIF") value of THB 1 or more are now subject to both customs duties and 7% value added tax ("VAT"). This policy shift will directly impact e-commerce, logistics, and retail sectors, and will have wide-ranging implications for any company involved in cross-border trade with Thailand.

Background

Under previous regulations, imported goods with a customs value (cost, insurance, and freight, or "CIF") of THB 1,500 or less were exempt from import duties. This was a cornerstone of the cross-border e-commerce model, allowing for the duty-free import of millions of small parcels.

Under the new policy, all imported goods, regardless of value, are now subject to assessment for import duties upon entry into Thailand. The stated rationale for this change is to create fair competition for Thai small and medium-sized enterprises ("SMEs"), which must pay VAT and other costs on their goods, putting them at a price disadvantage against foreign sellers who utilise the *de minimis* loophole.

Business Implications

This policy change will create new costs, compliance burdens, and operational challenges.

- a) **For foreign e-commerce sellers and platforms:** The most direct impact will be the addition of import duties to low-value items. Assuming the costs are passed on to the consumer, the higher prices and potentially more complex or slower customs clearance processes could lead to increased cart abandonment and reduced consumer demand. Businesses should review their pricing models and develop a clear strategy for calculating, declaring, and paying these new duties.
- b) **For logistics providers and customs brokers:** The administrative burden will be considerable. Carriers that previously handled millions of nondutiable parcels will now be required to process them for duty assessment and collection. This may necessitate new IT systems and streamlined processes to avoid delays at customs. The mechanism for duty collection (e.g., paid by carrier, paid by recipient) will be a critical operational detail.
- c) **For domestic SMEs and retailers:** The removal of the *de minimis* exemption is expected to bring increased competitiveness by narrowing the price gap between goods from Thai businesses and those from foreign competitors.

Outlook

Officials are exploring ways to simplify the tax process further. One proposal under review is a "lump-sum tax" system, which would apply a flat rate of 20 to 30 percent on all imported goods. However, implementing this system would require legislative amendments. The Customs Department has confirmed that the current policy complies with all existing international trade agreements, including Free Trade Area commitments, and is consistent with similar adjustments being made by other major economies worldwide.

Businesses involved in cross-border e-commerce should continue to:

- a) Assess the impact of the policy on product pricing and profit margins, using standard import duties based on HS (harmonized system) codes.
- b) Ensure their systems for product classification (HS codes) and valuation are accurate, as these are now critical for every shipment.
- c) Review and update pricing strategies and commercial models, and determine whether any system integrations are needed to support upfront tax collection.
- d) Monitor official announcements from the Ministry of Finance and Customs Department, including any developments regarding the proposed lump-sum tax system.

This policy marks a fundamental shift away from duty-free, low-value cross-border e-commerce in Thailand. Businesses that prepare for the new cost and compliance conditions will be best positioned to navigate the transition successfully.

CONTACT



Chitchai Punsan

Partner
Tilleke & Gibbins

T: +66 2056 5579

E: chitchai.p

@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

Technology and Intellectual Property Legal Update

The IP Puzzle of AI-Generated Songs: Protection, Responsibility, and the Future of Music Law

AI-generated songs are now making waves in Vietnam on platforms like TikTok, with tracks such as “*Say mot doi vi em*” quickly gaining popularity and sparking widespread attention. This phenomenon raises a host of legal and ethical questions: Who is the author of these songs? Can they be protected by copyright? Who is responsible if there is an infringement? These questions are becoming increasingly urgent as AI music becomes more mainstream in Vietnam.

Copyright Protection for AI-Generated Music in Vietnam

Under current Vietnamese law, copyright protection is reserved for works that bear the mark of human creativity. The 2022 amendments to Vietnam’s Intellectual Property Law reaffirm that only works created by humans are eligible for copyright. In practice, if a human meaningfully contributes to the creative process—by providing prompts, making selections, editing, or arranging—their contribution may be protected. However, if a song is generated entirely by AI without significant human input, it is unlikely to qualify for copyright protection.

When an AI-generated song does not qualify for copyright protection, the question arises as to whether the person who writes the prompts, edits, or compiles the work can still be considered the owner of an asset under the Vietnamese Civil Code. According to Article 105 of the Civil Code 2015, assets include objects, money, valuable papers, and property rights. While AI-generated music that is not protected by copyright is not considered money or valuable papers, it may be regarded as an object (in the form of a digital file or recording) or as a property right if it can be possessed, used, transferred, or exploited for value.

Use of AI-Generated Works Without Copyright Protection

If a song is not protected by copyright, does that mean anyone can use it freely? Not necessarily. The absence of copyright does not mean the work is entirely free of restrictions. Terms of service from AI platforms may limit commercial use, require attribution, or impose licensing fees. Other rights may also apply. The person who creates, edits, or compiles the AI-generated work may establish civil ownership over the digital file or recording as a type of digital asset, provided that the creation and use of the asset are lawful and do not infringe on others’ rights. This ownership is not the same as copyright, but it allows the owner to possess, use, and dispose of the asset within the limits of the law and any relevant agreements.

Additionally, laws against unfair competition, impersonation, or violations of personal rights (such as voice, name, or image) may still be relevant.

Voice Cloning and Related Risks

One particularly thorny issue is voice cloning. In Vietnam, performers’ rights protect both live performances and recorded voices. More importantly, copying or

imitating a singer's voice can primarily infringe upon the moral rights and personal rights of individuals as recognised under the Civil Code, which increasingly treats voice as a personal identifier. The main legal risk is the violation of moral rights, such as the right to protect the integrity and authenticity of one's voice and the right to be recognised as the owner of that voice.

Best practices include obtaining written consent from the person whose voice is used, labelling content as "AI voice," and avoiding any suggestion that the artist participated in or endorsed the work.

Similarity to Existing Works

Another significant risk arises when AI-generated music or lyrics resemble existing works. The standard for infringement is "substantial similarity" and access to the original. If an AI creates a segment that is sufficiently similar to a prior work, using that segment in a new recording or arrangement may constitute infringement. The fact that the AI was trained on large datasets does not exempt the output from scrutiny. Even if the input data was lawfully obtained, the output must still avoid copying protected material. Defences such as coincidence, common style, or minor excerpts are assessed on a case-by-case basis, often requiring expert analysis.

Responsibility and benefit-sharing in the AI music ecosystem are complex. Users who prompt, select, edit, or publish AI-generated music are directly responsible for the outputs they release or exploit. AI platforms may also bear responsibility if they provide infringing tools or models, or fail to remove infringing content. Those who invest in, release, or commercially exploit AI-generated music may profit under contract, but they also assume corresponding legal risks, including compensation, takedown, or recall obligations.

Practical Recommendations for Creators and Publishers

For creators and publishers, several practical recommendations emerge. It is important to document the human role in the creative process, demonstrating selection and editing to support claims of authorship.

- a) Similarity checks should be conducted using melody and lyric analysis tools, and expert opinions should be sought when necessary to avoid recognisable copying.
- b) Voice governance is critical: Do not clone an artist's voice without written consent, label AI-generated voices clearly, and avoid implying artist involvement.
- c) Use models and training data with clear provenance (noting that the 2025 IP Law amendment now permits use of legally published copyrighted materials for non-commercial AI training without a license under the TDM exception, though commercial use still requires full compliance with authors' and rights holders' rights) and keep records to prove origin.

- d) Internal contracts should allocate rights and responsibilities among authors, producers, singers, engineers, and publishers, including indemnity clauses for intellectual property claims.
- e) Platform terms should be reviewed carefully for output usage rights, commercial restrictions, and labelling obligations.
- f) Finally, establish procedures for receiving and responding to takedown notices promptly to minimise damage.

Legal Outlook in Vietnam

Vietnam is actively shaping its legal framework to address AI-generated content. The Law on Artificial Intelligence, which took effect on 1 March 2026, now requires that AI-generated audio, images, and video be machine-labelled, and that deployers clearly disclose when content is created or edited by AI if it could mislead the public about the authenticity of events or individuals. Crucially, for the music industry, the law expressly prohibits the collection or processing of data for AI training in violation of intellectual property law, and establishes a strict liability regime under which deployers of high-risk AI systems remain liable to compensate persons harmed even when operating in full regulatory compliance.

Also significant is the 2025 amendment to the IP Law, effective from 1 April 2026, which introduces a standalone text-and-data mining (TDM) exception. Under this exception, legally published and publicly accessible copyrighted works (including songs and recordings) may be used for AI training without a license, provided the use does not unreasonably affect authors' and rights holders' legitimate interests. Critically, the exception shields only the training process, not the outputs: if an AI model produces content "substantially similar" to a copyrighted song, infringement liability remains.

A draft decree amending Decree No. 17/2023/ND-CP on copyright is set to clarify the rules for AI-assisted creative works. Under the proposed rules, copyright will only arise when a human makes a "significant and decisive contribution", such as crafting prompts, evaluating and selecting outputs, or making final artistic decisions that ensure the result reflects the creator's own vision. Works generated entirely by AI will not qualify for copyright, and creators seeking registration for AI-assisted works must declare how AI was used. The draft decree also limits the use of copyrighted materials, including existing songs, for AI training to non-commercial research only, and rights holders may "opt out" of having their works used as training data altogether.

Key IP Takeaways on AI-Generated Content

AI-generated music challenges traditional IP frameworks on three fronts: authorship and protection, risks of voice cloning and similarity to prior works, and the allocation of liability among users, platforms, and publishers.

The safest path forward is proactive: Document the creative process, clear rights diligently, and use contractual safeguards. With these measures, businesses can treat AI not as a legal hazard, but as a sustainable creative tool in Vietnam's fast-evolving music landscape.

As Vietnam's evolving legal landscape offers both opportunities and uncertainties, stakeholders in the music and creative industries should stay informed and engaged with these regulatory developments to navigate the future of AI-generated content.

This article first appeared in [Managing Intellectual Property](#).

CONTACTS



Linh Duy Mai

Head of IP
Enforcement, Vietnam
T&G Law Firm LLC
(TGVN)

T: +84 24 3275 3958
E: duylinh.m@tgvn.vn



Diep Thi Bich Le

Senior Associate
T&G Law Firm LLC
(TGVN)

T: +84 24 3275 3935
E: diep.l@tgvn.vn

Technology Legal Update

Vietnam's New Personal Data Protection Law: A Closer Look

Vietnam officially enacted Law No. 91/2025/QH15 on Personal Data Protection (“**PDPL**”) on June 26, 2025. The PDPL took effect on January 1, 2026, along with a new implementing decree, and applies to (i) Vietnamese entities; (ii) foreign entities in Vietnam; and (iii) foreign entities directly involved in or related to the processing of personal data of Vietnamese citizens and persons of Vietnamese origin without a determined nationality, currently residing in Vietnam, who have been granted a personal identification certificate.

While the PDPL retains many provisions from its predecessor, Decree No. 13/2023/ND-CP on Personal Data Protection, it adds new concepts, exemptions, and compliance obligations. Notably, it sets out a framework regulation for penalties for violations, including monetary fines of up to 5% of the corporate violator’s annual revenue in the previous year for cross-border data transfer breaches.

The promulgation of the PDPL represents a major advancement in Vietnam’s legal landscape, reinforcing the existing data protection framework for better safeguarding the privacy and personal rights of Vietnamese citizens in the digital era, and at the same time promoting the digital economy and international integration in the country.

Some key takeaways from the PDPL are presented in this article.

Definitions of “Personal Data,” “Basic Personal Data,” and “Sensitive Personal Data”

The PDPL introduces broad definitions for “personal data,” “basic personal data,” and “sensitive personal data.” It expands the scope of personal data to include both digital and non-digital formats, such as paper-based records. Notably, de-identified personal data is explicitly excluded from the definition of personal data. The PDPL further delegates authority to the government to issue exhaustive lists specifying which types of data qualify as basic and sensitive personal data. These lists are expected to be detailed in the PDPL’s implementing decree.

Data Subjects’ Rights and Obligations

The PDPL retains the rights of data subjects as previously outlined in the Decree No. 13/2023/ND-CP on Personal Data Protection (“**PDPD**”), with clarifications of the rights themselves and certain strengthened procedural requirements. In addition to the data subjects’ rights, the PDPL imposes specific obligations on data subjects, including the obligations to:

- a) self-protect their own personal data;
- b) honor and protect others’ personal data;

- c) provide adequate and accurate personal data according to applicable laws and regulations, contracts, or consent given to the processing of their own personal data; and
- d) comply with the personal data protection laws and regulations and participate in the prevention of personal data infringements/violations.

These provisions are designed to prevent misuse of personal data rights and promote a culture of shared responsibility in the digital environment, while reinforcing individuals' control over their own data.

Personal Data Trading and Transfer

The PDPL strictly prohibits the sale and purchase of personal data, except as otherwise prescribed by the law. This prohibition is part of a broader effort to combat the widespread illegal online trading of personal data and prevent insider abuse. Violations of this provision may result in severe penalties, including fines of up to 10 times the revenue gained from the unlawful act of personal data trading.

The PDPL provides clarification, however, that certain types of data transfers do not constitute the "sale and purchase of personal data." These include:

- a) When the data subject has given consent.
- b) When data is shared between departments within the same agency or organisation for processing in line with the determined purpose.
- c) When data is transferred for continued processing due to the division, separation, or merger of agencies, organisations, or administrative units; the reorganisation or transformation of ownership of state-owned enterprises; the division, separation, merger, consolidation, or dissolution of entities or organisations; or the establishment of entities or organisations based on the dissolution of other entities or organisations.
- d) When the data controllers or data controller-processors transfer data to a data processor or third party (e.g., independent data controllers) for processing as prescribed.
- e) Upon request from competent state authorities.
- f) In circumstances where personal data can be processed without the data subjects' consent as prescribed under the PDPL (see item 5 below).

These exceptions are expected to be further detailed in the PDPL's implementing decree.

Maximum Administrative Sanctions for Violations

In addition to the maximum fine for illegal personal data trading, the PDPL sets the maximum administrative fine on an organisation for violations related to cross-border personal data transfers at 5% of the violator's revenue in the preceding fiscal year. In cases where the organisation has no revenue in the preceding year, or where the fine calculated based on such revenue is lower than VND 3 billion

(approx. USD 114,500), the latter will apply. The maximum administrative fine for other violations in the field of personal data protection is VND 3 billion. The method to calculate revenue arising from violation of personal data protection regulations will be further prescribed by the government under the PDPL's implementing decree.

Consent Requirements

The consent-centric approach and strict consent formality requirements of the PDPD are maintained in the PDPL, which provides additional cases of consent-exemptions. These include, among others, situations where personal data processing is necessary to protect one's own legitimate rights or interests, or those of others, as necessary against acts that infringe upon such interests (e.g., legal defence), and the fulfilment of contractual obligations not only of the data subjects but also of the service provider.

While the PDPL uses the term "legitimate interest," its scope is significantly narrower than under the General Data Protection Regulation (GDPR), and applies only when data processing is required to prevent infringement by third parties.

For situations where consent is exempted, the PDPL introduces a requirement for the data controllers and relevant data processors to implement a monitoring mechanism to protect the data, including but not limited to implementing appropriate data protection measures and regularly assessing possible risks, periodically inspecting and assessing compliance with the law, and receiving and addressing feedback and petitions from relevant parties.

The PDPL includes a transition clause allowing personal data processing activities that have been carried out prior to the effective date of the PDPL with the consent of the data subject or based on an agreement in accordance with the PDPD, to continue, without requiring new consent or a new agreement. This provision offers continuity for businesses already compliant with the PDPD, while signalling the need for updated practices that align with the PDPL's enhanced standards.

Data Processing and Data Transfer Impact Assessment

The requirements for the preparation, submission, and maintenance of a Data Processing Impact Assessment ("DPIA") and a Data Transfer Impact Assessment ("TIA") under the PDPD are inherited by the PDPL. The PDPL has assigned the government to provide detailed requirements on the dossier, conditions, order, and procedures for each impact assessment in the PDPL's implementing decree. However, it is anticipated that these requirements will generally align with those outlined in the PDPD.

To reduce the compliance burden, the PDPL makes it optional for small businesses and startups to comply with the DPIA requirements for five years from the PDPL's effective date, while household businesses and micro-enterprises are exempt. However, entities that provide personal data processing services, directly process sensitive personal data, or process the personal data of a large number of data subjects are not eligible for this exemption.

The PDPL mandates a six-month update cycle for both the DPIA and the TIA if there are any changes. Immediate updates are required in specific circumstances, such as (i) company restructuring, termination, dissolution, or bankruptcy; (ii) change of organisation or individual providing personal data protection services; or (iii) introduction of new business lines/activities or changes to the current business lines/activities involving personal data as declared in the DPIA and TIA.

DPIAs and TIAs received by the Cybersecurity and High-Tech Crime Prevention Department under the Ministry of Public Security (known as the “A05” department) before the PDPL’s effective date (i.e., January 1, 2026) in accordance with the PDPD will remain valid. However, any updates made to these dossiers made after the PDPL comes into force must comply with the requirements set out under the PDPL.

Notification of Violations

One of the key changes introduced by the PDPL is the revised timeline for notification of detected violations. Organisations are now required to report violations within 72 hours of detection, rather than from the time of occurrence as previously mandated under the PDPD. Moreover, while the PDPD only requires notification to the regulator (specifically, the A05), the PDPL expands this obligation to include notifying affected data subjects in cases involving biometric data incidents or incidents related to financial service providers.

Special Personal Data Protection Mechanisms

Some special data protection mechanisms are introduced under the PDPL, as follows:

For specific data subject groups: The PDPL sets out enhanced and more comprehensive safeguards for the personal data of vulnerable groups, such as children and individuals with limited or lost civil act capacity, or those with cognitive or behavioural impairments. For instance, the processing of children’s data generally requires only parental consent. However, if the data pertains to the child’s private life or personal secrets, and the child is age 7 or older, dual consent from both the child and the parent must be obtained.

For specific businesses and operational activities: The PDPL outlines tailored safeguards for personal data processing activities across various sectors and operational activities, including employment (recruitment and employee management); health data and insurance business; financial, banking, and credit information activities; advertising services; social network platforms and online communications services; big data processing, artificial intelligence, blockchain, virtual universe and cloud computing; and audio and video recording in public places and public activities. While some provisions are sector-specific, some can be generally applied to all enterprises; for instance, the requirement for deletion/destruction of information provided by job applicants who are not hired, unless there is a different agreement with the applicant.

For specific types of sensitive personal data: Specific safeguards required for processing location and biometric data are also prescribed under the PDPL.

Personal Data Protection Department and Personnel

The PDPL requires organisations to either designate a qualified department and personnel dedicated to personal data protection, or engage external data protection service providers. Such personal data protection departments, personnel, and service providers are components of what the PDPL refers to as the “personal data protection forces.”

While the government has yet to issue detailed regulations on “personal data protection forces,” further guidance on the conditions, responsibilities, and tasks of the designated data protection department and personnel are expected in the PDPL’s implementing decree.

Small and startup enterprises are granted a five-year grace period from the PDPL’s effective date to determine whether to comply, while household businesses and micro-enterprises are exempted from this requirement (save for cases where these entities provide personal data processing services, directly process sensitive personal data, or process the personal data of a large number of data subjects).

Outlook

The promulgation of the PDPL represents a major advancement in Vietnam’s legal landscape, reinforcing the existing data protection framework for better safeguarding the privacy and personal rights of Vietnamese citizens in the digital era, and at the same time promoting the digital economy and international integration in the country. Businesses will need to reevaluate and consolidate their data governance practices and internal controls to ensure prompt and effective PDPL compliance. It is also important for businesses to keep an eye on upcoming regulations and guidance to properly implement the PDPL.

CONTACTS



**Waewpen
Piemwichai**

Counsel
Tilleke & Gibbins

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



Quang Minh Vu

Associate
Tilleke & Gibbins

T: +84 28 6284 5661
E: quang.v@tilleke.com



**Hien Thi Thu
Nguyen**

Tilleke & Gibbins

T: +84 28 628 45678
E: vietnam@tilleke.com

DNA



Learn more
about us



Follow us on
LinkedIn

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