DREW NETWORK ASIA

ASEAN ROUNDUP



CONTENTS

NO.	COUNTRY	CONTENT	PAGE
1	Singapore	Singapore Introduces Model Governance Framework for Agentic AI	4
2	Singapore	Affirmation of Implied Term of Mutual Trust and Confidence *Prashant Mudgal v SAP Asia Pte Ltd* [2026] SGHC 15	12
3	Indonesia	Redrawing the Rules: Bank Indonesia's New Payment System Regime	18
4	Malaysia	Not Guilty yet Dismissed: Recent Industrial Court Decision Upheld Termination Despite Domestic Inquiry Findings	26
5	Laos	Laos Implements Online Registration System for Pharmaceutical Submissions	29
6	Myanmar	Preregistration Strategies for Safeguarding Trademarks in Myanmar	32
7	Myanmar	Myanmar Tightens Alcohol Control and Licensing	34
8	Thailand	Thailand Issues Guidelines on Digital Platform Fee Transparency and Fairness	38
9	Thailand	Thailand's Advertising Guidelines Targeting AI-Generated Content	42
10	Vietnam	Is Vietnam Pioneering the Legal Framework for AI and IP?	46
11	Vietnam	Industrial Design Protection for Locarno Class 32: A New Era in Vietnam	49

SINGAPORE

DREW & NAPIER LLC

Artificial Intelligence and Digital Trust Legal update

Singapore Introduces Model Governance Framework for Agentic AI

What is Agentic AI?

Agentic AI systems are systems that can plan across multiple steps to achieve specified objectives, using AI agents. Unlike generative AI, which requires a prompt to produce content, agentic AI can take actions, adapt to new information, and interact with other agents and systems to complete tasks autonomously.

The Model Governance Framework for Agentic AI (the "**MGFA**") focuses on agents built on language models. In summary, the language model functions as the "brain" of the agent, where it will receive instructions (from a human user) that can be in natural language and not in code, and analyse how to execute the instructions to achieve the objective. It will then (a) draw on repositories of information stored and available to the language model; as well as (b) draw on tools (e.g. calculator app, calendar app, web crawlers, etc.) linked to the language model to complete the task. If the language model is the "brain", the tools are the "arms and legs" that have received signals from the "brain", enabling the agent to perform actions and interact with other systems, such as controlling a device, or performing a transaction.

There are AI agents that are "deterministic", meaning that they produce consistent and identical outputs when given the same inputs, so their performance is predictable. There are also AI agents that are "non-deterministic", where they produce variable outputs even with the same input. This lack of predictability affects the level of confidence that can be placed in the agent's output, and how much human oversight is then required.[1]

It is common for an agentic system to have multiple agents working together, where each agent specialises in a certain task and work in parallel with other agents. The design of each agent will affect its limits and capabilities on 2 fronts:

a) Action-space (impacting authority and capabilities): The range of actions the agent can execute are determined by the tools it is permitted to access (e.g. sandboxed tools that cannot affect any other system, or an organisation's internal system, or external systems through third-party APIs) and the transactions it can execute (e.g. being able to read and retrieve information only rather than write and modify data in a system).

b) Autonomy (impacting decision-making): The degree to which the agent can decide when and how to act towards a goal is determined by its instructions (e.g. is it instructed to follow an SOP or can it exercise its own judgment) and level of human involvement in the agentic system.

[1]See section 2.1 of the World Economic Forum's "Agents in Action: Foundations for Evaluation and Governance" white paper (Nov 2025) https://reports.weforum.org/docs/WEF_AI_Agents_in_Action_Foundations_for_Evaluation_and_Governance_2025.pdf, referenced in footnote 3 of the MGFA.

Why does Agentic AI pose additional risk?

While agents are already transforming workplaces through coding assistants, customer service agents, and enterprise productivity workflows, their greater capabilities bring forth new risks. Some risks are already known to us and managed, such as the risks arising from the language models the agentic system is built on. However, these existing risks can manifest themselves differently, or compound themselves, due to the added capabilities of AI agents.

For example, a hallucination from an AI agent may result in a wrong plan to compete a task, and this mistake escalates where the initial wrong output is passed on to other agents - if an inventory figure from one agent is erroneous, a downstream agent might use this data and place an order for excessive or insufficient stock.

The MGFA highlights that organisations must be aware of these 5 risk categories:

Risk Category	Description
Erroneous actions	Incorrect actions such as an agent fixing appointments on the wrong date (resulting in harm due to delayed treatment) or producing flawed code (leading to exploitable security vulnerabilities).
Unauthorised actions	The agent takes actions outside its permitted scope or authority, like acting without escalating for human approval despite the SOP requiring it.
Biased or unfair actions	The agent's actions result in unfair outcomes across different profiles and demographics (e.g. in hiring decisions, or vendor selection).
Data breaches	Exposure or manipulation of sensitive data, including personal identifiable information or confidential information such as trade secrets and customer lists. For example, a security breach where attackers exploit the agent to reveal private information, or the agent discloses such sensitive information as it fails to recognise such information is sensitive.
Disruption to connected systems	Agents causing disruption to the systems they are connected to when they are compromised or malfunctioning, e.g. deleting a production codebase or overwhelming external systems with requests.

What best practices for organisations does the MGFA recommend to manage risk?

The MGFA establishes four key dimensions that organisations deploying agentic AI must address. This would apply whether the organisation is developing the AI agent in-house or using third-party developed agentic solutions.

Dimension 1: Assess and bound the risks upfront

Organisations should adapt their internal structures and processes to account for new risks from agents due to their adaptive and autonomous nature, and their

ability to directly impact the environment they operate in through taking actions (via the tools they are connected to).

a) **Step 1: Is this use case suitable for agent deployment based on the likelihood and impact of the risk:**

Organisations must conduct risk identification and assessment as the first step when considering whether to use agentic AI. The MGFA sets out the factors to consider when assessing risk, where it is a function of both:

(1) "Impact" (severity of impact if the risk manifests)	(2) "Likelihood" (probability of the risk manifesting)
• Level of tolerance of error in the domain and use case in which the agent is being deployed to. • Whether the agent can access sensitive data, such as personal information or confidential data. • Whether the agent can access external systems. • Whether an agent can only read from or modify the data and systems it has access to. • Reversibility of agent's actions.	• Agent's level of autonomy – a higher level of autonomy can result in higher unpredictability and increased likelihood of error. • How complex the task is (number of steps, level of analysis required at each step) – where a higher level of complexity increases unpredictability and thus the likelihood of error. • Agent's level of access to external systems and who the external systems are maintained by, as exposure to external systems makes the agent more vulnerable to prompt injections and cyberattacks.

b) **Step 2: After selecting an appropriate agent use case, further bound the risks by defining limits and permission policies for each agent:**

Design Boundaries: Organisations should limit the scope of impact of their agents by designing appropriate boundaries at the planning stage. This includes:

1. Defining policies giving agents only the minimum tools and data access needed to complete tasks.

2. Defining SOPs for agentic workflows that the agent must follow rather than granting the agent the freedom to define every step, to improve consistency and reduce unpredictability.

3. Designing mechanisms to take agents offline and limit potential scope of impact when they malfunction.

Agent Identity Management: Organisations should extend identity management to agents to track individual agent behaviour and establish who (e.g. which employee or department) is accountable for each agent. Each

agent should have its own unique identity, and authorisation should ensure that human users cannot set permissions for agents greater than what the human user is authorised to do.

Dimension 2: Make Humans Meaningfully Accountable

The MGFA makes it clear that "the organisations that deploy agents and the humans who oversee them remain accountable for the agents' behaviours and actions". This is despite the fact that agents can operate autonomously, and multiple stakeholders are involved across the agent lifecycle (both within and outside of the organisation).

Clear Allocation of Responsibilities Within the Organisation: Within the organisation, responsibilities should be allocated to different teams depending on their expertise, across the agent lifecycle:

a) Key decision-makers such as board members, department leaders (setting goals, defining permitted use cases, governance approach).

b) Product teams (design, implementation, testing, user education).

c) Cybersecurity teams (protecting agentic systems from cyber threats, managing security measures, incident response).

d) Any individuals using the output of AI agents (ethical use, compliance with organisational policies).

Clear Allocation of Responsibilities Outside the Organisation: This may be achieved through contractual means, as against the agentic AI system provider that provided the agentic system to the organisation. In turn, the agentic AI system provider would have upstream contractual arrangements with the model developers whose models it built the agents on, as well as other software and tool providers whose products are integrated.

Design checkpoints for meaningful human oversight: Organisations should define significant checkpoints or action boundaries requiring human approval, especially before sensitive actions are executed. These include high-stakes actions and decisions, irreversible actions (e.g. permanently deleting data, sending communications, making payments), outlier or atypical behaviour, and user-defined boundaries based on the user's risk appetite.

Audit Human Oversight: Organisations should also implement measures to ensure continued effectiveness of human oversight, including training humans to identify common failure modes (e.g. inconsistent agent reasoning or the agent referring to outdated policies) and regularly auditing the effectiveness of human approvals since humans are susceptible to automation bias.

Dimension 3: Implement Technical Controls and Processes

Organisations should implement technical measures across the agent lifecycle to ensure the AI agents operate safely and reliably.

During Development: Implement controls during the design and development phase to mitigate identified risks, in addition to baseline software and large language models ("**LLM**") controls. For example –

a) Where it comes to planning and reasoning, prompt the agent to summarise its understanding and request clarification from the user before proceeding.

b) Where it comes to tools, configure strict input formats and apply principle of least privilege, limiting the tools available to each agent.

c) Where it comes to protocols (a standardised way for an agent to communicate with tools and other agents), use standardised protocols where applicable, whitelist trusted servers and sandbox any code execution.

Before Deployment: Test agents for safety and reliability to ensure they will work as expected and that controls are effective. The starter kits for testing of LLM-based apps can be used as language models are a core component of agents, but new risks must also be covered, such as overall task execution accuracy, policy compliance, tool calling accuracy, and reactions to errors and edge cases. Testing should cover entire agent workflows, individual and multi-agent behaviour, and occur in realistic environments.

During and After Deployment: Gradually roll out agents into production to control risk exposure (e.g. to trained users first, with restricted tools initially, in lower-risk internal systems first). Continuously monitor and log agent behaviour, establishing reporting and failsafe mechanisms for failures or unexpected behaviours.

Dimension 4: Enable End-User Responsibility

Organisations cannot solely rely on their agentic system developers for successful deployment of agentic AI – they must also require their end-users to use agentic AI responsibly. An "end user" is the person that interacts with the agentic system, or who integrates the agent into their work processes. Therefore, organisations must provide sufficient information to the end users to enable their responsible use of the agentic system.

Transparency: Users should be informed upfront that they are interacting with an agent and not a human. They should also be informed of the agent's capabilities (e.g. what actions it can take, what user's data it can access), who to escalate the issue to if they suspect the agent is malfunctioning, as well as the user's own responsibilities (such as whether he/she must double-check all information provided by the agent).

Education and Training: Organisations whose employees are integrating agents into their workflows (e.g. coding assistants) should additionally provide training covering foundational knowledge on agents (use cases, prompting best practices), and how to have effective oversight of agents (common failure modes, common user mistakes). As agents take over entry-level tasks, organisations should ensure employees retain core skills through sufficient training and work exposure.

What can organisations do now?

While the MGFA does not impose binding legal obligations, it provides a clear picture of Singapore's regulatory direction for agentic AI and establishes industry best practices. Organisations can start with the following:

a) **Conduct a gap analysis:** Review current AI governance policies against the MGFA's four dimensions to identify areas requiring enhancement.

b) **Review vendor contracts:** Ensure contracts with agentic AI providers, model developers, and tooling providers adequately address security arrangements, performance guarantees, data protection, and liability allocation.

c) **Establish internal governance:** Work with technical teams to define appropriate use cases, set agent boundaries, establish human approval checkpoints, and implement monitoring mechanisms.

d) **Develop user policies:** Create acceptable use policies for employees using agentic AI and ensure appropriate training is provided.

e) **Monitor developments:** The MGFA is described as a living document that will be continuously updated and refined. Organisations should monitor for updates and prepare for potential future regulatory developments.

Please do not hesitate to contact any members of our Artificial Intelligence & Digital Trust Practice, if you require more information about the framework, or how Singapore's AI laws and guidelines presently apply to your business operations.

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



Benjamin Gaw

Director, Corporate Mergers & Acquisitions
Drew & Napier LLC

T: +65 6531 2393
E: benjamin.gaw @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



Cheryl Seah

Director, Corporate & Finance

T: +65 6531 4167
E: cheryl.seah @drewnapier.com



Albert Pichlmaier

Senior Cybersecurity and Privacy Engineer, Corporate & Finance

T: +65 6531 4108
E: albert.pichlmaier @drewnapier.com

Employment Legal Update

Affirmation of Implied Term of Mutual Trust and Confidence
Prashant Mudgal v SAP Asia Pte Ltd [2026] SGHC 15

Introduction

In *Prashant Mudgal v SAP Asia Pte Ltd* [2026] SGHC 15 ("**Mudgal**"), the employee brought a claim against the employer for: (a) breach of an implied term that the employer would not exercise its right to terminate the employment agreement arbitrarily, capriciously, perversely, irrationally, or in bad faith, (b) breach of the implied term of mutual trust & confidence (the "**ITMTC**"), and (c) conspiracy.

The High Court dismissed all of the employee's claims, save for the claim that the employer breached the ITMTC. However, the Court also held that the employee failed to prove any loss flowing from the breach of the ITMTC with the result that he only had a Pyrrhic victory.

Implied term exists under Singapore law

The case is of interest because the existence of the ITMTC in Singapore has not been clear in the last decade. In *The One Suites Pte Ltd v Pacific Motor Credit (Pte) Ltd* [2015] 3 SLR 695 (CA), the Court of Appeal remarked that the position of the ITMTC was "*still left open for decision in a future case*". In *Dong Wei v Shell Eastern Trading (Pte) Ltd* [2022] 1 SLR 1318 (AD) ("**Dong Wei**"), the Appellate Division said in *obiter* that "*the status of the [ITMTC] has not been clearly settled in Singapore*" and remains an open question for the Court of Appeal to resolve in a more appropriate case. Following *Dong Wei*, there have been three High Court decisions in which the ITMTC was considered. In two of them, the Court did not take a position on the existence of the implied term. In the most recent decision in *Dabbs, Matthew Edward v AAM Advisory Pte Ltd* [2024] SGHC 260, the Court found that the ITMTC does not exist under Singapore law. Since the Court in *Mudgal* was not bound by any of the preceding decisions, it was an opportunity for the Court to pronounce its own views on the existence of the ITMTC.

Despite the earlier questions about the existence of the ITMTC under Singapore law, the Judge found that the ITMTC exists under Singapore law.

First, the Judge took the view that there is ample precedent for the ITMTC in the Singapore High Court. The Judge noted that there were at least four High Court decisions prior to *Dong Wei* which alluded to or implicitly accepted the existence of the ITMTC. The Judge also noted that there were two subsequent High Court decisions where the Court did not take a position on the existence of the ITMTC, and only one where the Court stated in clearer terms that it was not minded to conclude that such an implied term existed in Singapore.

Second, the Judge's view was that the ITMTC is justified on principle. The Judge took the view that the implied term has taken a "life of its own" which could be applied in Singapore notwithstanding the absence of the specific legislative context which gave rise to it in the UK.

Finally, the Judge's view was that considerations of policy and fairness militate toward the implication of the ITMTC in Singapore law, since employment contracts were relational contracts which involved a continuing relationship of trust and confidence between the parties, unlike general commercial contracts. The Judge opined that the power imbalance between the employer and employee, coupled with the importance of a person's occupation to the individual meant that there was a greater need to afford protection to employees through the implication of the ITMTC.

For these reasons, the Judge held that the ITMTC serves to augment and sustain the trust and confidence between employer and employee that is vital to any employment relationship.

Scope of implied term

The Judge held that the "*lodestar*" for any Court applying the ITMTC is that an employer must not without reasonable and proper cause, conduct itself in a manner calculated and likely to destroy or seriously damage the relationship of confidence and trust between employer and employee.

The threshold which the employer's conduct must cross is a high one and requires "quite extreme behaviour" to satisfy the test. There is also no breach of the implied term if there is reasonable and proper cause for the employer to act in that manner, which means that an employer is afforded the opportunity to justify its actions.

However, the precise content of the ITMTC has to be determined on a case-by-case basis, and that the sub-duties identified in *Cheah Peng Hock* (e.g. duties not to act in a corrupt manner, not to unilaterally and unreasonably vary terms, and not to reprimand without merit in a humiliating circumstance) do not necessarily apply in all employment contracts under Singapore law.

The ITMTC must also not contradict an express term of the contract, and parties are free to modify or exclude its operation in their contract by express words to that effect.

On the other hand, the ITMTC does not restrict or fetter an employer's right to terminate an employment contract in accordance with the provisions of the contract. Indeed, the Judge found on the facts that there was nothing wrong with the employer's decision to terminate the employee's employment, which it had every right to do at any point in time, in accordance with the employment agreement.

Therefore, the Judge focused on the employer's conduct prior to the termination of the employee's employment. The Judge found that the employer had embarked on a performance improvement plan ("**PIP**")with a pre-ordained outcome, and in doing so had breached the ITMTC.

Contractual principles of damages apply

However, the Judge found that the damages sought by the employee were unsustainable at law and that the employee failed to prove any loss. The employee sought to claim damages amounting to $4,961,767.05 for the following three heads of losses: (a) continuing financial losses, (b) damages for pain and suffering and disamenities caused by Major Depressive Disorder ("**MDD**"), and (c) injury to his reputation.

The Judge held that the employee's claimed losses failed the contractual principles of causation and remoteness.

Continuing financial losses

The employee had claimed for loss of earnings from the date of his termination to the date that the suit was heard.

The Judge held that there was no basis for the employee to assert that he is entitled to his salary and/or salary increment. There is no right to specific performance of an employment contract or to require an employer to continue the employment relationship indefinitely. It was sufficient that the employer gave the employee more than the requisite notice under the employment agreement.

The Judge also found that the employer's conduct did not have any bearing on the employee's employability, and did not cause his inability to secure gainful employment after his termination.

Damages for pain and suffering

The Judge also rejected the employee's claim for damages for pain and suffering caused by his MDD.

The Judge did not accept that the employee's MDD damaged his employment prospects, and found that it was more likely that the employee could not secure a job because of other factors such as the COVID-19 pandemic.

In any case, the Judge found that the employee's claim was too remote to establish a claim in damages. There was no indication that the employee had a pre-existing vulnerability which the employer should have been aware of. In fact, the employer was never made aware of the fact that the employee was suffering from MDD.

Injury to reputation

The Judge also rejected the employee's claim for damages for injury to his reputation given that there was no causal link between the employer's conduct and the alleged losses. The employer's conduct did not affect the employee's ability to secure employment after his termination.

Given the Judge's finding that the alleged losses were not caused by the employer's conduct and were too remote, the Judge held that the employee failed to prove any loss flowing from the breach of the ITMTC and awarded nominal damages in the sum of S$1,000.

Comments and observations

The decision provides several learning points.

The High Court's judgment adds to the body of case law that has discussed the existence of the ITMTC in Singapore law, and is the first case to affirm the existence of the ITMTC under Singapore law following *Dong Wei*. The question remains ripe for appellate consideration, but the Court's forceful affirmation means that employers and employees will be prudent to guide their employment relationships on the basis that the ITMTC exists.

It is not uncommon for organisations to consider the PIP as a necessary human resource step before they take employment decisions that are adverse to an employee. The judgment in this case confirms that there is nothing to prevent an employer from exercising its contractual right to terminate employment without undertaking a PIP. Therefore, while the use of the PIP as a corrective measure may be well-intended, it is not an immutable checkpoint.

The High Court's judgment also brings welcome clarity on the appropriate remedial consequences which follow from a breach of an employment obligation during the period of employment, and a reminder that, even if there is a breach, that is not a licence to claim damages that fail to pass the usual contractual principles of causation and remoteness.

From a potential employee-claimant's perspective, the easy perception is that his employer's actions are responsible for his inability to replicate his previous status, remuneration and even confidence. However, this case is a stark reminder that an unprincipled approach to a claim that does not consider the legal principles for the award of damages will be fatal in a Court's assessment.

The authors are the employer's counsel. Views expressed in this article are those of the authors in their private capacities.

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



Kelvin Tan

Director, Director,
Dispute Resolution
Drew & Napier LLC

T: +65 6531 2526
E: kelvin.tan
@drewnapier.com



Benjamin Goh

Director, Director,
Dispute Resolution
Drew & Napier LLC

T: +65 6531 2424
E: benjamin.goh
@drewnapier.com



Kenneth Kwek

Senior Associate,
Dispute Resolution
Drew & Napier LLC

T: +65 6531 2597
E: kenneth.kwek
@drewnapier.com

INDONESIA

MAKARIM & TAIRA S.

Banking & Finance Legal Update

Redrawing the Rules: Bank Indonesia's New Payment System Regime

Bank Indonesia has introduced a new regulatory framework for Indonesia's payment systems industry, which took effect on 31 March 2026.

The new framework revokes previous "umbrella" regulation that had applied since 1 July 2021[1], while allowing existing rules for Payment Services Providers ("**PJP**") and Payment System Infrastructure Providers ("**PIP**") to remain in force, provided they are not inconsistent with the regime. The framework is set out in Bank Indonesia Regulation No. 10 of 2025 and its implementing regulation, Members of the Board of Governors Regulation No. 32 of 2025 (together, the "**Regulations**").

Parties that had obtained a PJP license or PIP designation before the Regulations took effect continued to be recognised as licensed providers. These entities (collectively, Payment Service Providers or "**PSPs**"), could also continue to apply existing operational standards, provided those standards do not conflict with the Regulations. The same approach applies to Supporting Providers (a party that conducts activities to support the operation of payment system services and/or payment system infrastructure carried out by PSP).

This Advisory highlights the key new provisions and Bank Indonesia's updated licensing approach introduced under the Regulations.

Recognised Activities

For PIPs, the changes introduced under the Regulations are not particularly significant, as a designation as a PIP continues to be granted for clearing activities and final settlement activities. More substantive changes are introduced in relation to PJPs.

Under the previous regulatory regime, Bank Indonesia categorised PJP licenses based on the scope of activities conducted by each PJP. Under the Regulations, this approach has been refined, rather than issuing licenses by type, Bank Indonesia now determines packages of PJP activities (bundling), structured around the specific activities carried out by the PJP.

[1]Bank Indonesia Regulation No. 22/23/PBI/2020 of 2020 on Payment Systems, Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment Services Providers, and Bank Indonesia Regulation No. 23/7/PBI/2021 on Payment System Infrastructure Providers

Each PJP must hold a license that reflects the relevant activity bundle applicable to its business model, as follows.

	Activities Engaged
Bundling Activity 1	This covers activities that are closest to the core handling of funds and the end-to-end processing of payment transactions, as follows. a) Administration of sources of funds, which includes: 1. administration of payment accounts; and 2. issuance and/or provision of access to source of funds b) Forwarding of payment transactions, which includes: 1. forwarding of payment transaction data and payment instructions, which may be accompanied by facilitation of receipt of payment proceeds through the provision of sub-accounts to merchants or service providers; and 2. forwarding of fund transfer instructions, whether conducted digitally or non-digitally. c) This bundle consists of two sub-packages: 1. Bundling Activity **1A**, which may only be carried out by PJPs that are classified as primary PSPs, reflecting the higher systemic importance and risk profile associated with these activities; and 2. Bundling Activity **1B**, which may be carried out by PJPs that are classified as non-primary PSPs.
Bundling Activity 2	This covers payment forwarding activities that do not include the administration of sources of funds. Specifically, this bundle consists of: a) forwarding of payment transaction data and payment instructions, which may be accompanied by facilitation of receipt of payment proceeds; and b) forwarding of fund transfer instructions, whether conducted digitally or non-digitally.
Bundling Activity 3	This covers the forwarding of non-digital fund transfer instructions.

Transaction, Interconnection, Competence, Risk Management, and Information Technology Infrastructure ("TIKMI") Assessment

The Regulations introduce the TIKMI assessment, a new assessment framework used by Bank Indonesia to evaluate a PSP's performance and to determine its classification as either a primary PSP[2] or a non-primary PSP.

From a procedural perspective, the TIKMI assessment begins with a self-assessment by the PSP, which must be submitted to Bank Indonesia within the prescribed timelines. Bank Indonesia will then conduct its own TIKMI assessment and formally determine the assessment results.

[2] *Primary PSP is a PSPs which, due to their size, interconnectedness, and complexity within the payment system or the financial system, may cause the failure of part or all the payment system and the financial system—either operationally or financially—if such PSPs experience disruptions or failures.*

A summary of the relevant frequency and deadlines of the TIKMI assessment is set out in the table below.

	Primary PSP	Non-primary PSP
Frequency	At least once every six months.	a) At least once every six months for the transaction and interconnection criteria; and b) at least once a year and at most once every three years for competence, risk management, and information technology infrastructure criteria.
Self-assessment Submission	a) 1 February, for assessment data covering July–December of the preceding year; and b) August, for assessment data covering January–June of the current year.	1 February, covering data for the January–December period of the preceding year.
Determination by Bank Indonesia	March and September	September

For PSPs that have not yet been classified as either primary or non-primary, the initial TIKMI assessment will be conducted in accordance with the assessment period applicable to non-primary PSPs. The initial determination of the TIKMI assessment results for PSPs will be made by Bank Indonesia no later than 1 April 2027 based on the self-assessment results submitted under the required period.

License Adjustments

Under the Regulations, Bank Indonesia will conduct an evaluation of the activities currently carried out by PSP. The evaluation will serve as the basis for determining the adjustment of activity bundling and the classification of PSPs, taking into account compliance with the licensing requirements applicable to PSPs, and the results of the TIKMI assessment.

Based on the outcome of this evaluation, Bank Indonesia will:

a) align the activities attached to an existing PJP license or PIP designation obtained before the Regulations take effect with the relevant activity bundles (for PJPs) or activities (for PIPs) as regulated under the Regulations; and

b) reclassify existing classification of PJPs and PIPs that were previously designated as systemic, critical, or general payment system operators into the new PSP classifications of primary PSP or non-primary PSP.

Bank Indonesia will communicate the results of this evaluation in writing to the relevant PJP or PIP no later than one year from the effective date of the Regulations, i.e. by 31 March 2027.

SBP and RBSP Submission

Another key new feature introduced under the Regulations is the requirement for PSPs to prepare and submit a Strategic Business Plan ("**SBP**") and Payment System Business Plan ("**RBSP**") to Bank Indonesia.

Both documents must be submitted to Bank Indonesia, but they are subject to different regulatory treatments. The SBP will be reviewed by Bank Indonesia which may request revisions, while the RBSP will require formal approval from Bank Indonesia.

The first submission of SBP and RBSP were to be made no later than 30 April 2026. Thereafter, both must be submitted annually by 30 November. The standard reporting format for the SBP or RBSP has been released by Bank Indonesia.

A PSP may amend its submitted SBP once a year, with any amendment reflected in the corresponding RBSP. The RBSP may also be amended once a year, provided that the amendment is submitted no later than the end of the business day in June of the relevant RBSP period.

The SBP is prepared for a three-year period and must at least include the following matters:

a) vision, mission, and strategic direction;
b) analysis of the business environment, opportunities, and challenges;
c) management policies and strategies;
d) implementation of risk management;
e) business activity plans and strategic development plans; and
f) financial projections, including transaction projections.

Meanwhile, the RBSP is prepared for a one-year period and must at least include the following matters:

a) results of supervision by the Board of Commissioners;
b) accountability of the Board of Directors;
c) changes to the SBP;
d) realisation of the RBSP for the previous period; and
e) business activity plans and development plans.

The first SBP to be submitted must cover the 2026–2028 period, while the first RBSP must apply for the 2026 period.

Ongoing Capital

Under the Regulations, PSPs are required to comply with ongoing capital requirements, broadly in line with the previous payment systems regulatory regime. While the overall framework remains familiar, the Regulations introduce adjustments to the capital thresholds, particularly through the additional capital surcharges based on a PSP's risk profile as follows:

For PJP	For PIP
a) 1.5% of risk-weighted transactions for PJPs with a transaction and interconnection assessment rating of moderate to high; and b) 2.5% of risk-weighted transactions for PJPs with a transaction and interconnection assessment rating of high.	a) 2.5% of risk-weighted transactions for PIP with a transaction and interconnection assessment rating of moderate to high; and b) 5% of risk-weighted transactions for PIP with a transaction and interconnection assessment rating of high.

Notwithstanding the adjustments to the capital thresholds, the composition of ongoing capital remains broadly consistent with the previous Bank Indonesia regulatory framework.

Cooperation with Supporting Providers

Under previous Bank Indonesia regulations, cooperation with Supporting Providers was governed by a risk-based approach. Under the new Regulations, Bank Indonesia refines this approach by introducing a clear categorisation of Supporting Providers as follows.

a) Critical Supporting Providers, i.e. those providing supporting services to primary PSPs and/or PSPs other than primary PSPs, above a certain threshold value;

b) Important Supporting Providers, i.e. those provide supporting services to PSPs other than primary PSPs, above a certain threshold value; and

c) Standard Supporting Providers, i.e. those providing supporting services that are not related to the stages of payment transaction processing, which include initiation, authorisation, clearing, and final settlement.

To strengthen the supervision on the key third-party arrangements, the Regulations require Critical Supporting Providers and Important Supporting Providers to be registered with Bank Indonesia, or another party appointed by Bank Indonesia, within three years from the effective date of the Regulations, i.e. by 31 March 2029. In line with this, a PSP may only cooperate with a Critical or Important Supporting Provider that has been duly registered.

The Regulations also introduce a more structured approval regime for product developments and third-party cooperations. A PSP must obtain Bank Indonesia's approval for any development or cooperation that affects the payment transaction processing (which consists of initiation, authorisation, clearing, and final settlement), as well as pre-transaction and post-transaction activities. For this, a PSP must refer to the RBSP that has been approved by Bank Indonesia.

Depending on the nature of the development, approval is obtained either through:

a) an approval mechanism for complex developments and developments that result in an increase in the activity package (bundling); and

b) a reporting mechanism for standard developments which must be submitted at the latest 10 working days after the implementation date of the development and cooperation.

Following implementation, the PSP is required to report the realisation of the approved development and cooperation, with relevant supporting documents, to Bank Indonesia. This reporting must be made through the RBSP for the subsequent period and no later than 10 business days after the commencement of the relevant activity and cooperation.

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

CONTACTS



Maria Sagrado

Partner,
Makarim & Taira S.

T: +6221 5080 8300, 2521272
E: maria.sagrado@makarim.com



Budhy Apriastuti Evita

Senior Associate,
Makarim & Taira S.

E: budhy.apriastuti@makarim.com



Kaila Arinta Nazneen Z

Associate,
Makarim & Taira S.

E: kaila.nazneen@makarim.com

MALAYSIA

SHEARN DELAMORE & CO.

Employment & Industrial Relations Legal Update

Not Guilty yet Dismissed: Recent Industrial Court Decision Upheld Termination Despite Domestic Inquiry Findings

In the recent case of **Mohd Dzulkarnain Bin Shaharud-Din v TM Technology Services Sdn Bhd** (Award No. 245 of 2026), the Industrial Court reaffirmed the well-established principle that an employer is not bound by the findings of a domestic inquiry panel, even where the domestic inquiry panel has found the employee not guilty of the charges preferred.

In this case, the domestic inquiry panel exonerated the claimant of the charges of misconduct against him. However, the employer's disciplinary committee disagreed with the domestic inquiry panel's findings and proceeded to dismiss the claimant for misconduct. The claimant argued that the dismissal was unfair due to the "*not guilty*" finding by the domestic inquiry panel.

The Industrial Court rejected the claimant's argument and clarified several important principles. A domestic inquiry is primarily a fact-finding mechanism, and its findings are not final or binding on the employer. The employer retains the inherent power to differ from the domestic inquiry panel's conclusion, provided it applies its mind to the evidence and records reasons for its disagreement.

Further, the Industrial Court emphasised that proceedings before it are heard *de novo*. As such, the Industrial Court is not concerned with the correctness of the findings made by the domestic inquiry panel. Instead, the Industrial Court's task is to determine, based on the totality of the evidence adduced before it, whether the employer has established the alleged misconduct on a balance of probabilities, and whether such misconduct amounts to just cause or excuse for dismissal.

Importantly, while the Industrial Court acknowledged that an employer should not lightly disregard a *"not guilty"* finding by the domestic inquiry panel, it confirmed that such a finding does not immunise an employee from dismissal.

This Industrial Court decision serves as a timely reminder that employers may lawfully terminate employment despite an exonerating domestic inquiry outcome, provided the decision is reasoned, supported by evidence and capable of being justified before the Industrial Court.

Contact us for further information regarding employment and industrial relations matters.

Copyright © 2026 Shearn Delamore & Co. All rights reserved.

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

CONTACT



Hua Zhi Loon

Senior Legal Associate
Shearn Delamore & Co.

T: +603 2027 2874
E: vijayan@
shearndelamore.com

LAOS

TILLEKE & GIBBINS

Regulatory Affairs Legal Update

Laos Implements Online Registration System for Pharmaceutical Submissions

Laos' Food and Drug Department ("**FDD**") has been using a new online registration system for drugs since the beginning of the year. The system, which was implemented following the November 2025 issuance of Notice No. 5960/FDD, became the official pathway for submissions on January 1, 2026. Since that date, paper-based registrations have no longer been accepted. This marks a significant advancement in the digitalisation of regulatory processes in Laos.

As the online system is now the exclusive platform for registration, renewal, and amendments, companies that have not yet aligned their processes to the new system should act promptly to ensure a smooth transition. To assist with this, the FDD will conduct periodic training sessions on the use of the online registration system, which will be delivered either in person or remotely, depending on operator demand.

To start using the system, drug and medical device manufacturers, as well as import-export companies, that have not yet registered must submit a formal request identifying the authorised personnel (the "**Designated User**") who will access the platform, after which they will be issued user accounts and access codes. Each request must be accompanied by the company's enterprise registration certificate (incorporation certificate), a copy of the identity card or passport of each Designated User, and a scanned copy of their signature. There is no restriction on the number of Designated Users per company, allowing flexibility to meet operational needs.

Companies that already hold accounts and access codes from the trial phase may continue using them and may apply for additional accounts if needed.

Additional Requirements

The new system also introduces a standardised format for drug registration numbers. For example, an import drug registration number such as 06 I 4040/15 will be changed to 06-IM-04040-15, and a domestic drug registration number such as 06 L 4040/15 will be changed to 06-LM-04040-15. Companies are required to update packaging to reflect the new format within two years and must report progress periodically to the FDD.

For pharmaceutical products that require sample analysis prior to registration or renewal, manufacturers or companies must send samples directly to the National Food and Drug Analysis Center and upload the sample receipt into the online system.

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

Intellectual Property Legal Update

Preregistration Strategies for Safeguarding Trademarks in Myanmar

Myanmar's Trademark Law 2019 (the "**Trademark Law**") introduced a modern framework for the registration, enforcement, and protection of trademarks. However, due to the high volume of applications filed during the soft-opening period of the Intellectual Property Department ("**IPD**"), marks submitted from 2022 onward remain pending as the IPD works its way through the applications filed in 2021, which it has been publishing on a monthly basis since May 1, 2024. During this period, businesses should adopt proactive strategies to protect their brands, monitor conflicting marks, and ensure a smooth registration process.

Practical Steps for Safeguarding Pending Marks

While a pending application does not confer full trademark rights, brand owners can take several practical steps to strengthen their position:

a) **Monitor IPD publications.** Businesses should regularly review the IPD's monthly gazette to identify any identical or confusingly similar marks at an early stage and prepare timely oppositions in accordance with the Trademark Law's provisions allowing "any interested party" to file an objection to a trademark application.

b) **Monitor market activity.** Early detection of potential infringement enables swift action, such as cease-and-desist letters and opposition proceedings. Businesses should monitor competitors, distributors, and retailers for unauthorised use of their marks.

c) **Collect evidence of use.** Maintaining evidence of use strengthens claims of distinctiveness and supports enforcement efforts. Businesses should keep records of commercial activities, distribution, brand promotion and development, marketing communications, product packaging and labeling, and sales demonstrating brand recognition in Myanmar and internationally, particularly in Southeast Asian markets. Although the Trademark Law establishes a first-to-file system, evidence of use provides considerable practical support for distinctiveness claims and enforcement actions.

d) **Pursue Interim Enforcement Options.** A pending trademark application can be relied upon to oppose or refuse other marks on absolute and/or relative grounds of refusal. In addition, marks with established reputations may be protected under passing-off principles or unfair competition provisions in applicable statutes. Interim remedies to deter misuse are available prior to formal registration.

e) **Consider Priority Claims.** Where applicable, brand owners should consider claiming priority through the WTO route to secure an earlier filing date and prevent intervening applications from undermining established claims.

f) **Prepare in Advance for IPD Examination.** Brand owners should anticipate potential objections on absolute or relative grounds, including descriptiveness, lack of distinctiveness, or similarity, and prepare supporting

evidence in advance. Proactive preparation helps ensure a smoother examination process and reduces the risk of delays.

Conclusion

Although Myanmar's trademark procedures continue to evolve, the application stage need not leave brand owners exposed. A pending application is not a passive phase—it can be actively safeguarded through monitoring, evidence collection, and interim enforcement. Priority claims and advance preparation for examination further strengthen protection and reduce delays.

Safeguarding trademarks in Myanmar begins well before the certificate of registration is issued. Pending marks are valuable assets when managed strategically—particularly with tailored local advice that considers options for monitoring, evidence preparation, and enforcement options to ensure brands remain protected throughout the application process.

CONTACTS



Niko Myint Soe

Associate
Tilleke & Gibbins

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



Khin Zar Chi Kyaw Win

IP Consultant
Tilleke & Gibbins

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

Regulatory Affairs Legal Update

Myanmar Tightens Alcohol Control and Licensing

Myanmar has introduced a comprehensive new regulatory framework for alcoholic beverages that will impose stricter controls on production, distribution, advertising, and sales. On March 7, 2026, the National Defence and Security Council issued a new Excise Law (NDSC Law No. 13/2026), repealing the Excise Act of 1917. The law, which has not yet entered into force, will take effect on a date to be specified in a separate notification—likely within this year.

The new Excise Law establishes clearer definitions, introduces multiple categories of excise licenses and permits, and significantly expands prohibitions and compliance obligations for businesses operating in the alcohol sector. Many operational details will be clarified through implementing rules and notifications.

Scope and Definitions

The new law defines "excise" to cover alcoholic liquor and excisable articles. Alcoholic liquor is broadly defined as any liquid containing more than 0.5% ethyl alcohol, including beer, wine, toddy sap, fermented liquor, and any other liquid declared as alcohol by notification of the relevant ministry, excluding denatured alcohol. Alcoholic liquor is further categorised into country liquor, foreign liquor, and international-standard domestically produced liquor.

Excise Licensing

The law also introduces a more detailed licensing regime. The following types of liquor excise licenses are available:

a) Production
b) Production of value-added products
c) Bottling
d) Distribution
e) Sales
f) Other excise-related businesses designated by General Administrative Department ("**GAD**") notification

The GAD will prescribe the licensing fees, requirements, and conditions for each category through notifications issued with the approval of the Ministry of Home Affairs. The GAD may also, with the approval of the Ministry of Home Affairs, prescribe quantities and volumes of alcoholic beverages that may be possessed without a liquor license. No such prescribed quantities have yet been issued.

Holders of excise licenses for manufacturing, production of value-added products, or bottling must obtain approval from the relevant government department or organisation certifying that the alcoholic beverage is suitable for consumption.

Excise License Eligibility

The following entities may apply for licenses:

a) Myanmar citizens, associate citizens, or naturalised citizens under the Myanmar Citizenship Law.

b) Companies registered in Myanmar under the Myanmar Companies Law, including Myanmar-owned companies, foreign companies with foreign shareholding of up to 49%, wholly Myanmar-owned entities, business organisations formed by Myanmar citizens, or joint venture organisations.

Regardless of the date of issuance, all excise licenses are valid only until the end of the Myanmar government's financial year (March 31) and require annual renewal.

Additional Permits and Operational Requirements

In addition to excise licenses, the law introduces several permit requirements.

a) Factory permits are required for factories manufacturing alcoholic liquor, beer, or wine.

b) Transportation permits are required when license holders wish to transport alcoholic beverages to another licensed distributor or retailer.

c) Storage permits are required if alcoholic beverages are stored at premises other than those approved under the excise license.

d) Export rights are available to holders of manufacturing, production as value-added products, or distribution licenses, subject to compliance with applicable laws.

e) Import rights are limited to distribution license holders.

Key Prohibitions

The law imposes extensive restrictions:

a) Alcoholic beverages must not be sold or given to religious personnel, persons of unsound mind, or persons under the age of 18.

b) Selling alcoholic beverages online or through automatic vending machines is prohibited.

c) Advertising alcoholic beverages by any means—including signboards, flyers, displays, or similar methods—is prohibited.

d) Promotional activities for alcoholic beverages such as discounts, free samples, lucky draws, or gifts are prohibited.

e) Possession of alcoholic beverages in excess of prescribed quantities without a license is prohibited.

f) Retail excise license holders must not employ or allow female employees to work at a place where alcoholic beverages are sold.

Practical Implications

Although the new Excise Law is not yet effective, it signals a move toward stricter regulation of alcoholic beverages in Myanmar. Businesses involved in the alcohol sector should review their operations and compliance arrangements in preparation for implementing rules and notifications, particularly in relation to license categories, import and distribution controls, advertising and promotion restrictions, employment-related prohibitions, and annual license renewals. Further guidance is expected through subordinate legislation.

CONTACT



Kyaw Min Tun

Associate
Tilleke & Gibbins

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

THAILAND

TILLEKE & GIBBINS

Technology Legal Update

Thailand Issues Guidelines on Digital Platform Fee Transparency and Fairness

Thailand has introduced new regulatory guidance requiring digital platform operators to adopt structured, transparent, and fair fee practices. On March 16, 2026, the Electronic Transactions Development Agency ("**ETDA**") published Announcement No. DPS 2/2569, titled "Guidelines for Transparency and Fairness in Digital Platform Service Fee Determination," issued under the Royal Decree on Digital Platform Service Business Operations B.E. 2565 (2022). The guidelines establish a framework governing how digital platform operators should set, disclose, and adjust fees charged to users and related service providers such as logistics and payment providers.

Although framed as best-practice guidance rather than legally binding rules with explicit penalties, the guidelines carry regulatory weight under the royal decree and represent a significant step toward structured governance of digital platform fee practices in Thailand.

The guidelines establish various transparency principles and divide fees into two distinct categories—compulsory and additional—with specific governance principles for each.

Transparency Principles

The guidelines recommend that digital platform operators adopt several transparency measures to ensure that users can fully understand the costs of using a platform.

a) **Fee catalog**. All fees should be consolidated into a single, accessible location, which should include the fee name, definition, scope of covered services, calculation methodology, rate, billing period, and calculation examples.

b) **Minimum service disclosure**. Operators should disclose the minimum service that users can expect, such as baseline visibility, product listing capabilities, access to transaction data, and back-end dashboard access.

c) **Price structure disclosure**. Operators should disclose the categories of costs underlying their fees, such as system maintenance, cybersecurity, and operational costs. While exact cost figures need not be made public, operators should be able to provide numerical data to regulators upon request.

d) **Clear fee formulas**. Fee calculations should be simple and easy to understand—for example, percentage of net sales, cost per order, or cost per product listing. Operators should avoid multilayered or stacked fee formulas that may mislead users.

e) **Advance notice**. Operators should notify users at least 15 days in advance of any fee change, disclosing the reason, scope, potential impact on users, and channels for inquiries and feedback.

Compulsory Fees

Compulsory fees cover services essential to basic platform operations, such as transaction processing, payment systems, identity verification, back-end systems, security, and basic customer service. Key recommendations include the following:

a) **"1 activity = 1 fee" principle**. Each fee should correspond to a clearly defined service scope, with no double-charging.

b) **Cost-based logic**. Fees should be justifiable by reference to cost categories, though detailed cost figures need not be publicly disclosed.

c) **Minimum service guarantee**. Users who pay compulsory fees are entitled to stable systems, baseline visibility, basic customer support, and access to essential data.

d) **No conditional linkage**. Basic rights should not be degraded if a user declines to purchase advertising or add-on services. For example, product visibility should not be reduced for users who do not purchase advertising.

Additional Fees

Additional fees include value-added services such as advertising, sales promotions, and subscription packages that enhance business performance beyond the baseline. Governance recommendations for additional fees include the following:

a) **No impact on core benefits**. Declining add-on services should not reduce baseline visibility or degrade basic system performance.

b) **Value-based pricing**. Fees should reflect measurable outcomes, such as impressions or search ranking improvement.

c) **Optional, not mandatory**. The purchase of add-on services should be voluntary, with no coercive bundling or pressure to purchase.

d) **Unbundling principle**. Basic and add-on services should not be mixed in ways that force users to purchase unnecessary bundles.

Common Principles for All Fee Types

Regardless of category, the guidelines recommend several overarching principles applicable to all fees:

a) **Minimum service standards**. Each fee type should be linked to clearly defined minimum service levels, including baseline data access, standard visibility, and appropriate service periods.

b) **15-day public consultation**. Before any fee adjustment, operators should open a minimum 15-day consultation period, which should be accompanied

by a summary of key issues, impacts, and the operator's response to any feedback.

c) **Fee challenge mechanism**. Operators should maintain a formal process allowing users to dispute fees, with clear timelines, response procedures, and reasoning.

d) **Fair exit**. Cancellation procedures, especially for monthly or annual subscriptions, should be clear, reasonable, and free of excessive penalties.

Implications for Digital Platform Operators

Under the new guidelines, digital platform operators—particularly e-commerce marketplaces, food delivery apps, and similar intermediary platforms—may need to make significant operational and legal adjustments, and should review their current fee structures, disclosure practices, and terms of service for alignment with these guidelines. Key priorities include the following:

a) Preparing a consolidated fee catalog;
b) Developing advance-notice and consultation procedures for fee changes;
c) Implementing fee-dispute mechanisms; and
d) Ensuring internal cost-allocation records can be produced for regulators on request.

In addition, the "1 activity = 1 fee" principle and unbundling requirements may force operators to unbundle existing combined fee packages and justify pricing with cost-based or value-based rationale. The prohibition on conditional linkage, such as suppressing product visibility for users who do not buy ads, directly limits a common monetisation strategy and may affect revenue models.

CONTACTS



Athistha (Nop) Chitranukroh

Partner
Tilleke & Gibbins

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



Thammapas Chanpanich

Senior Associate
Tilleke & Gibbins

T: +66 2056 5561
E: thammapas.c@tilleke.com



Rada Lamsam

Associate
Tilleke & Gibbins

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



Karnravee Jitvilai

Associate
Tilleke & Gibbins

T: +66 2056 5709
E: karnravee.j@tilleke.com

Consumer Products & Technology Legal Update

Thailand's Advertising Guidelines Targeting AI-Generated Content

Thailand's AI legislative framework took another step forward when the Office of the Consumer Protection Board ("**OCPB**") issued a notification establishing guidelines for AI-generated advertising that may cause material misunderstanding about products or services. The notification, which is already in effect, was issued under the Consumer Protection Act B.E. 2522 (1979) and its amendments, which prohibit advertising that is unfair to consumers or may cause harm to society, including false or exaggerated statements and statements that may cause material misunderstanding about products or services.

The notification addresses emerging advertising practices, including the use of images edited using software or AI to attract consumer interest or build credibility. The OCPB noted that such advertising may result in consumers misunderstanding the essential characteristics, condition, or usage of products, which violates consumer rights and causes damage.

Key Requirements on AI-Generated or Digitally Manipulated Advertising Content

For advertisements using still images or videos created or edited with software programs or AI tools that may cause the depicted product or service to differ from the actual product sold or service provided—which may cause misunderstanding regarding the condition, quality, quantity, or other essential aspects of the products or services—advertisers and business operators must comply with the following requirements:

a) **Prior authorisation**. Obtain approval from relevant regulatory authorities where required by law.

b) **Accurate representation**. Ensure that the advertised size, quantity, volume, number, or composition matches the actual product or service being sold, whether in still images or videos.

c) **Mandatory AI disclosure labels**. Display clear disclosures when AI or software is used to create or edit images, such as:

1. "Real image or simulation edited using AI"
2. "Photo from actual location or simulation edited using AI"
3. "Photo from actual product or edited simulation"
4. "Image created by AI"
5. "Video created by AI"

d) **Clarity of disclosure**. Ensure disclosures are clearly visible, audible, or readable according to the type of advertising medium.

Recommendations

Business operators should assess their current advertising practices and update internal policies to ensure compliance with these new disclosure and warning requirements. Companies should ensure that marketing contracts and creative workflows incorporate the mandatory disclosures specified in the announcement. In particular, operators that develop, use, or rely on AI systems in their marketing activities should assess their current data governance practices and oversight mechanisms. Businesses should also monitor the ongoing development of Thailand's broader AI regulatory framework to ensure timely compliance with future requirements.

CONTACTS



Athistha (Nop) Chitranukroh

Partner
Tilleke & Gibbins

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



Thammapas Chanpanich

Senior Associate
Tilleke & Gibbins

T: +66 2056 5561
E: thammapas.c@tilleke.com



Rada Lamsam

Associate
Tilleke & Gibbins

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



Karnravee Jitvilai

Associate
Tilleke & Gibbins

T: +66 2056 5709
E: karnravee.j
@tilleke.com

VIETNAM

TILLEKE & GIBBINS

Intellectual Property Legal Update

Is Vietnam Pioneering the Legal Framework for AI and IP?

Vietnam's Law on Intellectual Property (IP Law) has undergone continuous amendment in recent years, with the latest amendment issued at the end of 2025. Among the amended and supplemented provisions, the regulation that has perhaps attracted the most attention is a provision relating to the use of protected IP objects by artificial intelligence (AI) systems.

Specifically, Article 7 of the 2025 IP Law introduces a completely new Clause 5, which reads in full as follows:

> *"Organisations and individuals are permitted to use texts and data relating to intellectual property objects that have been lawfully published, and which the public is allowed to access, for the purposes of scientific research, experimentation, and training of artificial intelligence systems, provided that such use will not unreasonably affect the legitimate rights and interests of the authors and intellectual property rights holders in accordance with this Law.*
>
> *With respect to texts and data that are objects protected by copyright and related rights, the use of the texts and data as set forth herein must also be in accordance with the regulations of the Government."*

Analysing this newly added provision in the context of how it was conceived, as well as the challenges that still lie ahead, can provide some interesting insights.

From Aspirations to Flight in Science and Technology

From the end of 2024 and throughout 2025—the 50th anniversary of the country's reunification—Vietnam witnessed numerous sweeping changes in many areas, including legislative development. It could be said that no sessions of the National Assembly have ever adopted as many laws, resolutions, and major policies as this one. The aspirations of the highest-level leadership have been concretised into major law and policy projects, which were drafted, developed, and passed at record speed.

All of this was aimed at building a foundation for Vietnam to achieve breakthrough development, with an expected GDP growth rate of up to 10% per year over the next decade. As a key driver of this growth, science and technology were given special attention, and the legal framework in this sector, including IP law, was urgently developed and amended.

Vietnam has not been hesitant to introduce new regulations, unprecedented even in developed countries, and establish the relationship between IP and AI with these goals in mind.

Caution in Building the Legal Framework

In this context, the question of whether the relationship between IP and AI should be incorporated into the amended 2025 IP Law became a topic of attention and debate from the outset, with two distinct approaches.

Legal scholars and practicing lawyers tended to be cautious about the idea of incorporating regulations governing the relationship between IP and AI into law, especially provisions relating to the use of protected IP objects by AI systems. Legal practitioners favored a more prudent approach, hoping that Vietnam would not move too hastily and would instead take time to observe and evaluate advanced legislative models worldwide. However, significant momentum came from upper leadership and the technology sector, who sought a legal corridor providing the most favorable conditions for tech companies to develop.

Even the tech companies themselves could not converge upon one consistent approach. Content-producing companies, whose rights and interests are closely tied to the control of the use of their works, tended to have the view that the use of protected IP objects must be subject to prior authorisation by the rights holders. Meanwhile, the companies which business models rely heavily on access to data welcomed and actively promoted a trend allowing them to freely use such objects even if they were protected by IP law.

Ultimately, the form of the provision that was adopted partially reflects the prevailing influence of the tech companies, as the 2025 IP Law officially introduced a principle allowing AI systems to "*use texts and data relating to intellectual property objects … provided that such use will not unreasonably affect the legitimate rights and interests of authors and intellectual property right holders*."

However, caution continues to be reflected in the final sentence of Article 7.5, which adds the key clause that *"With respect to texts and data that are objects protected by copyright and related rights, the use […] must also be in accordance with the regulations of the Government."*

Thus, the current regulation chosen by Vietnam could be deemed to be both open and closed. It is open in that it clearly sets out the principle that AI systems can use protected IP objects without prior consent from the right holders. However, the use of objects protected by the specific form of copyright and related rights – the form of IP protection most likely to apply to online content accessed by AI systems – will be implemented in accordance with regulations yet to be issued, which could close off certain avenues in the future. For now, pending the issuance of such regulations, AI systems can enjoy the rights already recognised.

Vietnam's legal provisions in this area appear to be of a pioneering nature. However, only time will tell if this is truly the case.

This article first appeared in Managing Intellectual Property.

CONTACT



Loc Xuan Le

Principal,
T&G Law Firm LLC
(TGVN)

T: +84 24 3275 3959
E: loc.l@tgvn.vn

Intellectual Property Legal Update

Industrial Design Protection for Locarno Class 32: A New Era in Vietnam

Vietnam's Intellectual Property ("**IP**") Law, despite being amended in 2022, underwent another significant revision at the end of 2025. The latest amendment aimed to address five major policy objectives set by the Vietnamese government, including promoting innovation, digital transformation, and international integration.

Among the most notable changes in the 2025 IP Law, which took effect on 1 April 2026, is the expansion of industrial design protection under Article 4.13. The revised definition now includes partial designs and intangible designs, marking a transformative shift in Vietnam's industrial design regime.

This change has particularly significant implications on designs classified under Class 32 of the Locarno Classification—which covers graphic designs, logos, ornamentation, surface patterns, arrangements, and other intangible products. These designs, previously excluded from protection in Vietnam, are now recognised under the new legal framework.

Background: Status of Class 32 Designs Before 2026

The Intellectual Property Office of Vietnam had previously applied the 13th edition of the Locarno Classification for industrial design filings. However, not all classes in this system had historically been eligible for protection. Under the 2022 IP Law, Class 32 designs were explicitly excluded based on the following legal grounds:

a) Definition under Article 4.13 (2022 IP Law): *"An industrial design is the external appearance of a product or a component for assembly into a complex product, expressed in shapes, lines, colors, or a combination thereof, and visible during the exploitation of the product's utility or the complex product."*

b) Product requirements under Article 21.2 of Circular 23/2023/TT-BKHCN: A product is defined as an object, a tool, a device, or means, manufactured by industrial or handicraft methods, with clear structure and function. A component for assembly into a complex product must be *capable of independent circulation* and detachable from the complex product.

Based on these definitions, Class 32 designs, such as graphical user interfaces ("**GUIs**") were excluded because they could only circulate with the devices with which they were associated. Applications for such designs were thus typically rejected during the formality examination stage, prior to publication.

In earlier years, when the exclusion of intangible designs was not clearly defined, applicants often attempted to modify their filings to fit eligible categories. For example:

a) A logo design (Class 32) could be reclassified as a label design (Class 19).

b) An ornamental pattern (Class 32) could be converted into a decorative material sheet (Class 11).

However, the IP Office later prohibited such practices by rejecting priority claims due to subject matter change and rejecting amendments that changed the nature of the original design.

The rationale for excluding intangible designs was never explicitly stated, but some opinions attributed it to practical difficulties in identifying, examining, and enforcing rights for such designs.

The 2025 Amendment: A Paradigm Shift Effective 1 April 2026

Under the amended 2025 IP Law, Article 4.13 introduces a broader definition: *"An industrial design is the external appearance of the whole or a part of a physical or non-physical product, expressed in shapes, lines, colors, or a combination thereof, and visible during the exploitation of the product's utility."*

This change expands protection to:

a) Partial designs (inseparable parts of products); and
b) Intangible designs (e.g., GUIs, digital patterns, virtual objects).

This amendment represents a major evolution in Vietnam's industrial design protection system, driven by the objectives of (i) adaptation to technological advancements—particularly the rise of digital and electronic products; (ii) alignment with global trends in industrial design protection; and (iii) enhanced applicant rights and incentives for creativity in design innovation.

While the expansion will undoubtedly create challenges in drafting guidelines, examination procedures, enforcement, and dispute resolution, it is considered a necessary step to meet the government's policy goals and respond to the rapid pace of societal and technological change.

Outlook

The inclusion of Class 32 designs under Vietnam's IP Law marks a significant milestone, opening the door for protection of intangible designs such as GUIs, logos, and digital patterns. This progressive move not only harmonises Vietnam's IP framework with international standards but also fosters innovation in the digital economy.

As implementation unfolds, design applicants can file and obtain protection for their partial designs and Class 32 designs in Vietnam. Moreover, refusals of such designs filed internationally under the Hague Agreement should no longer pose an issue.

This article first appeared in Managing Intellectual Property.

CONTACT



Thanh Phuong Vu

Counsel and Head of Patent, Vietnam
Tilleke & Gibbins

T: +84 24 3772 5571
E: phuongthanh.v@tilleke.com

DNA

Learn more about us

Follow us on LinkedIn

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