Legal 500
Country Comparative Guides 2025

Thailand
TMT

Contributor

CHANDLER MORI HAMADA

Chandler Mori Hamada Limited

Panupan Udomsuvannakul

Partner | panupan.u@mhm-global.com

Wongsakrit Khajangson

Partner | wongsakrit.k@mhm-global.com

Koraphot Jirachocksubsin

Counsel | koraphot.j@morihamada.com

Suphakorn Chueabunchai

Senior Associate | suphakorn.c@morihamada.com

Tatchai Luangphatarawong

Associate | tatchai.l@morihamada.com

Thanachart Osathanondh

Associate | thanachart.o@morihamada.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Thailand.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Thailand: TMT

1. Software – How are proprietary rights in software and associated materials protected?

Proprietary rights in software are protected through intellectual property laws, particularly the Copyright Act B.E. 2537 (1994) (as amended) (the "Copyright Act"). The Copyright Act provides automatic protection for the expression of original works of authorship, including computer software. Under the Copyright Act, software—referred to as a "computer program" —is defined as a set of instructions or anything used in conjunction with a computer to enable its operation or to generate an output, irrespective of the programming language used. Software is classified as, and protected under, the same category as literary works. Consequently, the Copyright Act primarily ensures the protection of the software's source code. To establish evidence of ownership, software owners have the option (but not the obligation) to notify the Department of Intellectual Property (the "DIP") of their copyright.

2. Software – In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

When determining the ownership of a copyright work, the Copyright Act does not differentiate between a software developer and a consultant. Instead, ownership depends on the nature of the arrangement, i.e., whether it constitutes (1) an employment relationship or (2) a hire of work arrangement. If software is developed by a developer during their employment with a company, the ownership of the software will vest in the developer, unless otherwise agreed in writing. However, the employer retains the right to communicate the work to the public in accordance with the purpose of the employment. On the other hand, if the software is developed by a developer on commission (hire of work), the copyright vests in the hirer, unless otherwise agreed. Therefore, it is crucial for the parties involved to establish a clear agreement that addresses copyright right ownership to avoid any uncertainty.

3. Software – Are there any specific laws that govern the harm / liability caused by Software / computer systems?

There are no specific laws that exclusively address harm or liability arising from software or computer systems.

Generally, the relevant laws may include, but are not limited to:

1. the Unsafe Goods Liability Act B.E. 2551 (2008) (Product Liability Act) and the Consumer Case Procedure Act B.E. 2551 (2008) – these laws provide a framework for addressing harm and liability caused by products, including software and computer systems. To establish liability, an injured party (consumer) generally must demonstrate that they suffered harm or damage while using the defective product in its intended manner. Similar to consumer protection regimes in many countries, these laws allow injured parties to pursue legal recourse by shifting the burden of proof regarding fault or negligence to the business operator; and
2. the Civil and Commercial Code – This may also apply more broadly, particularly in cases involving tort and breach of contract, to address liability arising from software or computer systems, i.e., covering matters outside the scope of consumer cases.

4. Software – To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

The specific law governing offenses related to the misuse of software and computer systems in Thailand is the Computer-related Crime Act B.E. 2550 (2007) (as amended) (the "Computer Crime Act"). This Act specifically penalizes activities such as unauthorized access to computer data (hacking), phishing, and the use of software as a tool to cause harm or damage to another person or their property.

5. Software Transactions (Licence and SaaS) – Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a

software vendor and customer, including any laws that govern the use of cloud technology?

There are no technology-specific laws that govern the provision of software between a software vendor and a customer in Thailand. The Civil and Commercial Code generally governs the contractual relationships of the transactions.

6. Software Transactions (License and SaaS) – Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

Yes, it is typical for a software vendor to cap its financial liability. As the majority of software is provided by foreign software houses, the cap typically reflects the standard terms adopted by such software houses.

7. Software Transactions (License and SaaS) – Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

As a majority of software is provided by foreign software houses, the cap typically reflects the standard terms adopted by such software houses. The areas of liability listed above are typically subject to negotiation to determine whether liability will be capped at all and, if so, how it will be capped.

8. Software Transactions (License and SaaS) – Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

No, it is not normal practice in Thailand.

9. Software Transactions (License and SaaS) – Are there any export controls that apply to software transactions?

Yes, the dual-use export control regime under the Control of Items in Relation to the Proliferation of Weapons of Mass Destruction Act B.E. 2562 (2019) also applies to software and technology.

10. IT Outsourcing – Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

Except for certain specific industries (e.g., financial institutions, digital asset business providers) which are subject to IT outsourcing requirements, there are no specific laws governing IT outsourcing transactions in Thailand.

11. IT Outsourcing – Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

There are no specific laws governing IT outsourcing transactions in Thailand.

12. Telecommunications – Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The principal laws governing telecommunications networks and services include the Organisation to Assign Radio frequency and to Regulate the Broadcasting and Telecommunications Services Act B.E. 2553 (2010) (as amended) (the "NBTC Act") and the Telecommunications Business Act B.E. 2544 (2001) (as amended) (the "Telecom Business Act"). The NBTC Act provides a comprehensive definition of "Telecommunications Service", while the Telecom Business Act sets out the licensing requirements for telecommunications business operators.

13. Telecommunications – Please summarise any licensing or authorisation requirements applicable to the provision or receipt of telecommunications services in your country. Please include a brief overview of the relevant licensing or authorisation regime in your response.

Under the NBTC Act and Telecom Business Act, telecom licenses are classified into three types as follows:

1. Type 1 License: granted to telecommunications business operators who operate telecommunications services without their own network, for services deemed appropriate to be fully liberalized, such as data center, cloud computing, internet, etc;
2. Type 2 License: granted to telecommunications business operators who operate telecommunications services with or without their own network, for services provided to a limited group of people, or services that do not have a significant impact on free and fair competition or on public interest; and
3. Type 3 License: granted to telecommunications business operators who operates telecommunications services with their own network, for services provided to the general public, or services that may cause a significant impact on free and fair competition or on public interest, or services that require special consumer protection, such as mobile network services.

14. Telecommunications – Please summarise the principal laws (present or impending) that govern access to communications data by law enforcement agencies, government bodies, and related organisations. In your response, please outline the scope of these laws, including the types of data that can typically be requested, how these laws are applied in practice (e.g., whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

The Computer-Related Crime Act B.E. 2560 (2017) (as amended) (the "**CCA**") provides the legal framework for addressing offenses committed in the digital realm and establishes rules and guidelines for the investigation, prosecution, and punishment of cybercrimes. The CCA also require service providers to retain certain data related to computer-related crimes for a specified period, facilitating the investigation and prosecution of cybercriminals.

Under the CCA, the Ministry of Digital Economy and Society (the "**MDES**") may request access to, or conduct investigates involving computer systems, computer traffic data, and user data in connection with criminal investigations. Furthermore, the MDES can order the production of any data or devices and seize computer systems where necessary. Depending on the nature of the enforcement, the competent officer must notify the competent court within 48 hours of exercising such authority.

Other relevant safeguards include restricting the duplication of computer data to circumstances where there are reasonable grounds to believe that an offence has been committed and ensuring that such actions do not unduly interfere with the operations of the owner or possessor of the computer data. In the case of seizure or attachment, in addition to providing the owner or possessor of the computer system with a copy of the document evidencing the seizure or attachment as proof, the competent officer may not order the seizure or attachment for more than thirty days unless specifically approved by the court.

15. Mobile communications and connected technologies – What are the principle standard setting organisations (SSOs) governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

There is currently no specific standard setting organisation governing the use and development of mobile communications and connected technologies in Thailand. However, these technologies are subject to oversight by various governmental authorities, each with distinct areas of responsibility. For example, the National Broadcasting and Telecommunications Commission ("**NBTC**") oversees telecommunications as outlined in our response to item no.13 above. The processing of personal data through connected devices, particularly in contexts such as health monitoring, falls under the jurisdiction of the Office of the Personal Data Protection Committee ("**PDPC**"). Furthermore, if mobile communications and connected technologies are related to applications, websites, or other digital platforms, compliance with the Royal Decree on Operation of Digital Platform Services Which Require Notification B.E. 2565 (2022) ("**Royal Decree on Digital Platform**"), regulated by the Electronic Transactions Development Agency

("**ETDA**"), may be necessary.

16. Mobile communications and connected technologies – How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Currently, there are no specific technical standards that govern mobile communications and connected devices in Thailand, so regulations regarding the interoperability of such technologies have yet to be established. However, devices that fall within the regulatory scope of the NBTC must adhere to the standards set by the NBTC for respective devices.

17. Data Protection – Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

The PDPA is Thailand's principal data protection legislation, modelled closely on the EU General Data Protection Regulation (GDPR). It is designed to safeguard personal data by regulating its collection, use, disclosure, storage, and processing. The PDPA establishes a broad framework of responsibilities for entities and individuals handling personal data, including obligations to provide privacy notices, obtain valid consent, and implement appropriate security measures to ensure data integrity and confidentiality. Failure to comply with the PDPA may result in civil, criminal, and administrative penalties.

18. Data Protection – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

The PDPA imposes a maximum administrative fine of THB 5 million for a violation of its provisions. In terms of criminal penalties, offenders may face imprisonment of up to one year and/or a fine of up to THB 1 million, depending on the nature of the offence. However, civil penalties, including both actual damages and punitive damages, are not subject to a fixed statutory cap as they vary depending on the specific circumstances of each case.

Apart from the PDPA, a newly enacted Emergency Decree on Measures for the Prevention and Suppression of Technology Crimes (No. 2) B.E. 2568, effective on April 13, 2025, imposes far harsher penalties specifically for the unlawful buying or selling of personal data. Under this decree, individuals found guilty may face imprisonment for up to five years and/or fined up to THB 500,000.

19. Data Protection – Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

No, typically, technology contracts do not directly incorporate external data protection regimes, but such regimes are sometimes referred to in data processing agreements or data sharing agreements.

20. Cybersecurity – Please summarise the principal laws (present or impending), if any, that that govern cybersecurity (to the extent they differ from those governing data protection), including a brief explanation of the general purpose of those laws.

The Cybersecurity Act B.E. 2562 (2019) ("Cybersecurity Act") is the principal legislation specifically governing cybersecurity in Thailand. Its overarching objective is to safeguard Thailand's cyberspace by establishing a comprehensive legal framework for the prevention, management, and mitigation of cybersecurity threats. The Act is particularly focused on entities responsible for information and communication infrastructure that is critical to national security and the public interest (CII). These include organisations involved in, or providing, national security, essential public services, banking and finance, information technology and telecommunications, transportation and logistics, energy and public utilities, and public health services.

Entities designated as Critical Information Infrastructure organisations are subject to a range of obligations under the Cybersecurity Act, including:

- The requirement to implement a code of practice covering all topics prescribed by the National Cybersecurity Committee (NCSC).
- The obligation to establish and maintain cybersecurity measures in accordance with standards set by the NCSC.
- The duty to notify the Office of the NCSC and other relevant regulators upon detection of any actual or potential cyber threats.

In addition, the NCSC has recently introduced cybersecurity standards for cloud systems. These standards are primarily aimed at organisations subject to the Cybersecurity Act, including cloud service providers providing services to such organisations. The objective is to minimise cyber risks associated with the use of cloud services by these entities.

21. Cybersecurity – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable cybersecurity laws?

The Cybersecurity Act imposes a maximum fine of THB 200,000 for administrative penalties, whereas the Act provides for a maximum penalty of three years' imprisonment for criminal penalties.

22. Artificial Intelligence – Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

Currently, there is no existing law or specific body that specifically governs the use of artificial intelligence ("**AI**"). However, a public hearing on the draft Royal Decree on Artificial Intelligence System Service Business (the "**Royal Decree on AI**"), proposed by the Office of National Digital Economy and Society Commission, was conducted in late 2022.

Additionally, a new draft principles on Artificial Intelligence (the "**Draft Principles on AI**") by the MDES recently underwent a public hearing process.

23. Artificial Intelligence – Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

The draft Royal Decree on AI aims to regulate service businesses utilizing AI, adopting a risk-based approach and focusing on two distinctive categories: prohibited AI and high-risk AI, similar to the EU's model. Prohibited AI refers to the use of AI that aims to influence or alter human behaviour, resulting in potential bodily or mental harm, or unfair discrimination that is disproportionate. Examples include AI employing subliminal techniques, social scoring, and real-time remote biometric identification systems used in public spaces. On the other hand, high-risk AI includes the use of AI that may result in unfair treatment or impact the rights or freedoms of others, such as the use of CV-scanning tools or test scoring systems. The use of prohibited AI is generally prohibited unless, for example, the AI systems are used under the supervision of specific regulators, while the use of high-risk AI must be registered with the competent authority.

Meanwhile, the Draft Principles on AI focus on establishing a legal framework for the development and application of AI, considering risks that may arise from uses that does not align with AI governance. It empowers authorities to collaborate in identifying prohibited or high-risk AI applications. Additionally, it imposes obligations on AI service providers, such as appointing a legal representative in Thailand and reporting serious incidents. The draft also affirms key legal principles, such as non-discrimination, and promotes measures such as exceptions for the use of copyrighted data and the adoption of AI testing sandboxes. It also provides for the establishment of the AI Governance Clinic to support the practical implementation of the law.

24. Artificial Intelligence – Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI (including agentic AI)?

No, there are currently no specific legal provisions in that respect. However, it is noteworthy that the Royal Decree on AI contains provisions relating to AI chatbots and deepfakes, requiring service providers and/or content creators to inform users of chatbot programs or viewers of deepfake content that they are interacting with AI or viewing artificially created content, as the case may be.

25. Artificial Intelligence – Do technology contracts in your jurisdiction typically contain either mandatory (e.g. mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

In Thailand, technology contracts do not typically include provisions regarding AI risks, as the use and development of AI are not yet widespread in the country. However, Thailand's future approach to AI is expected to align with international standards, such as the EU AI Act. Therefore, it is advisable that any provisions regarding AI risks in technology contracts should be designed to align with relevant global standards to ensure compliance and

maintain relevance, as the adoption of AI in Thailand increases.

26. Artificial Intelligence – Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Similar to the above response, as AI development in Thailand is still in its nascent stage, comprehensive legislation specifically addressing various aspects of AI has not yet been established. At this stage, in the absence of Thai laws on AI, it would be beneficial to include provisions in any agreements related to AI systems, including those regarding intellectual property rights, that are in line with relevant international practices.

27. Blockchain – What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

There are currently no laws governing blockchain technology in general.

As for digital assets, the Emergency Decree on Digital Asset Businesses B.E. 2561 (2018) is the primary law regulating both the offerings of digital tokens, commonly known as "initial coin offerings" ("**ICOs**"), and the undertaking of digital-asset-related businesses and activities. The purpose of this law is to enhance the standards for the digital asset market and safeguard stakeholders, particularly investors in the market. For example, token issuers must file a prospectus and obtain approval from the SEC prior to conducting an ICO. Additionally, certain digital asset business operators are required to obtain licenses before commencing their operations. These operators include: (i) digital asset exchanges, (ii) digital asset brokers, (iii) digital asset dealers, (iv) digital asset advisory service providers, (v) digital asset fund managers, (vi) initial coin offering portals, and (vii) digital asset custodial wallet providers.

28. Search Engines and Marketplaces – Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

The principal laws related to search engines and marketplaces include the Electronic Transactions Act B.E. 2544 (2001) (the "**Electronic Transactions Act**"), the Direct Sale and Direct Marketing Act B.E. 2545 (2002) (the "**Direct Sale Act**"), the Royal Decree on Digital Platforms, and the Consumer Protection Act B.E. 2522 (1979).

The Electronic Transactions Act establishes the legal framework for electronic transactions and provides guidelines for the use of electronic data messages. While it may not specifically govern search engines and marketplaces, it forms the legal foundation for the enforceability and admissibility of electronic evidence in Thai legal proceedings.

The Direct Sale Act regulates "direct marketing activities", particularly those conducted through online channels, where customers can complete a purchase order on a platform without any input from the platform operator, e.g., via carting systems. B2C e-commerce marketplace operators that meet these criteria must obtain direct marketing registration from the Office of the Consumer Protection Board (the "OCPB") under the Direct Sale Act. In addition, they are required to comply with other obligations such as preparing a return policy, submitting periodic reports, and maintaining a certain amount as a business guarantee with the OCPB.

The Royal Decree on Digital Platforms imposes obligations on digital platform service providers, including online marketplaces and search engines. The decree aims to regulate and monitor digital platform service providers that provide services to consumers in Thailand, regardless of the provider's legal residency or domicile. Operators of such platforms are required to comply with certain obligations such as notification to the ETDA prior to commencing their businesses, preparation of annual reports, disclosure of terms and conditions, and appointment of coordinators in Thailand.

Additionally, the draft Digital Platform Economy Act, which completed its public hearing in February 2025, aims to regulate the digital platform economy in Thailand, ensuring fair competition, consumer protection, and balanced oversight. It introduces obligations for digital platform service providers, including transparency, complaint mechanisms, advertising disclosures, and clearly stated terms of service. It also introduces a distinct category, "very large online platforms" (VLOPs), defined based on revenue, user base, or systemic risk, and subject to additional duties such as annual reporting, user tracking mechanisms for commercial transactions,

and prompt suspension of illegal activities. The draft Act also outlines the responsibilities of the "gatekeepers"—dominant service providers in core digital services—requiring open access, data sharing, and non-discriminatory practices.

29. Social Media – Please summarise the principal laws (present or impending), if any, that govern social media and online platforms, including a brief explanation of the general purpose of those laws?

Social media platform operators, as digital platform service providers, are required to comply with notification requirements, among other obligations, under the Royal Decree on Digital Platforms. The CCA, which is the main legislation governing social media in Thailand, aims to address a range of computer-related offences. These include offenses committed through social media platforms, such as spreading false information or sharing altered images of individuals intended to defame or humiliate them.

30. Social Media – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable online safety laws?

There are no dedicated online safety laws applicable to social media in Thailand. However, depending on the nature of the breach, sanctions under relevant laws may apply (e.g., the CCA, the Electronic Transactions Act, the PDPA, etc.)

31. Spatial Computing – Please summarise the principal laws (present or impending), if any, that govern spatial computing, including a brief explanation of the general purpose of those laws?

There are currently no dedicated laws specifically governing spatial computing in Thailand. However, several existing and forthcoming laws are relevant, and may apply, to certain aspects of spatial computing, primarily through their regulation of digital platforms, data, and online content, as outlined below:

- PDPA – Spatial computing applications frequently process personal data, including biometric, location, and behavioural data. The PDPA therefore applies to these technologies by protecting individuals' privacy rights and regulating the collection, use, and disclosure of personal data.
- Cybersecurity Act – Spatial computing platforms and services, particularly those integrated into critical sectors, may be classified as operators of critical information infrastructure and thus fall within the scope of the Cybersecurity Act. This imposes obligations relating to cybersecurity risk management and incident response.
- CCA – This Act grants the government authorities broad powers to regulate online content and activities, including those taking place within virtual environments. It is used to address issues such as online fraud, misinformation, and other computer-related offences that may arise in the context of spatial computing.
- Draft Royal Decree on AI – As spatial computing may rely on AI-driven technologies such as object recognition, motion tracking, and real-time data processing, the draft Royal Decree on AI—currently undergoing public consultation—may significantly impact the development, deployment, and operation of spatial computing solutions in Thailand. While the decree is not yet enacted, it is expected to introduce regulatory requirements concerning AI system transparency, accountability, risk assessment, and data governance, which spatial computing providers may need to comply with in the future.

32. Quantum Computing – Please summarise the principal laws (present or impending), if any, that govern quantum computing and/or issues around quantum cryptography, including a brief explanation of the general purpose of those laws?

There are currently no dedicated laws specifically governing quantum computing or quantum cryptography in Thailand. However, several existing and forthcoming laws could be relevant to the regulation of quantum computing or quantum cryptography, similar to those discussed in item 31.

33. Datacentres – Does your jurisdiction have any specific regulations that apply to data centres?

Thailand does not have a single, dedicated law that exclusively governs data centres. Instead, the operation, construction, and management of data centres are regulated through a combination of sector-specific laws and general regulatory frameworks, including the

following:

- Telecommunications business – Data centres are generally classified as designated businesses under the Telecommunications Business Act B.E. 2544 (2001). Operators are required to obtain an operating licence from the Office of the National Broadcasting and Telecommunications Commission (NBTC) before commencing operations. Most data centre activities typically fall under the scope of a Type 1 operating licence.
- BOI promotion – The Thai government actively encourages investment in data centre infrastructure through the Board of Investment (BOI). Under the Investment Promotion Act B.E. 2520 (1977), data centre operations are recognised as a promoted business activity. Operators may apply for a range of tax and non-tax incentives, such as corporate income tax exemptions, import duty exemptions, land ownership rights, and permission to employ foreign experts. To qualify for these benefits, data centre operators must satisfy specific conditions and requirements set by the BOI, including minimum facility size and investment thresholds.
- Environmental and Construction Regulations – Data centre often involve a large-scale development and must therefore comply with local building codes, environmental regulations, and utility requirements, particularly those related to energy and water usage.
- Sector-Specific Regulations – Data centres serving regulated industries (e.g., banking, insurance, healthcare) may be subject to additional requirements imposed by sectoral regulators.

34. General – What are your top 3 predictions for significant developments in technology law in the next 3 years?

We anticipate the following significant developments.

1. AI – Thailand is on the cusp of enacting comprehensive legislation to regulate the use and development of AI across various sectors. Multiple draft laws are already at an advanced stage, with strong indications that at least one will be enacted in the near future. The government's commitment is further underscored by the National AI Strategy and Action Plan, which sets out a structured roadmap for responsible AI adoption and governance.
2. Data Centres – As data centres become an increasingly vital part of Thailand's digital infrastructure, the development and establishment of a more comprehensive and robust legal framework to govern their operation is expected.
3. Digital assets – Relevant authorities are likely to collaborate to level the playing field between (i) various types of digital assets and (ii) their corresponding traditional securities equivalents. Notably, the Thai government is also taking a more active role in this sector, signaling its intention to participate directly in the digital asset market.

35. General – Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

No, it is not yet common for technology contracts in Thailand to include provisions related to environmental commitments or obligations. Nevertheless, the growing awareness and importance of Environmental, Social, and Governance (ESG) considerations among Thai companies suggest a potential future trend, and such provisions are expected to become more prevalent in the near future.

Contributors

Panupan Udomsuvannakul
Partner
panupan.u@mhm-global.com

Wongsakrit Khajangson
Partner
wongsakrit.k@mhm-global.com

Koraphot Jirachocksubsin
Counsel
koraphot.j@morihamada.com

Suphakorn Chueabunchai
Senior Associate
suphakorn.c@morihamada.com

Tatchai Luangphatarawong
Associate
tatchai.l@morihamada.com

Thanachart Osathanondh
Associate
thanachart.o@morihamada.com