COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

Thailand

TMT

Contributor

Chandler MHM

Wongsakrit Khajangson

Partner | wongsakrit.k@mhm-global.com

Panupan Udomsuvannakul

Counsel | panupan.u@mhm-global.com

Nonthagorn Rojaunwong

Senior Associate | nonthagorn.r@mhm-global.com

Shaswat Weeramongkolkul

Associate | shaswat.w@mhm-global.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. Is there a single regulatory regime that governs software?

No, Thailand does not have a dedicated regulatory regime specifically or exclusively governing software. The laws and regulations that apply to a particular software-related matter will vary depending on the specific facts and circumstances involved. These may include intellectual property laws, computer-related crime laws, product liability laws, as well as general principles of tort and criminal laws.

2. How are proprietary rights in software and associated materials protected?

The 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. The Copyright Act defines software, referred to as a "computer program", as a set of instructions or anything used with a computer to enable its operation or generate an output, irrespective of the programming language used. Software is classified 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.

3. 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 analysing the ownership of copyright work, the Copyright Act does not differentiate between a software developer and consultant. Instead, it depends on the type of arrangement, i.e., the nature of the (1) employment and (2) hire of work. If software is developed by a developer during the duration of his employment with the 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 employment. On the other hand, when software is developed by a developer on commission (hire of work), the copyright vests in the hirer, unless otherwise agreed upon. Therefore, it is crucial for the parties involved to establish a clear agreement, addressing the ownership of copyright right to avoid any ambiguity.

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

There are no specific laws that may apply to the harm or liability caused by 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) must prove that they suffered harm or damage while using the defective product in its intended manner. Similar to consumer protection laws in many countries, these laws allow injured parties to pursue legal recourse by shifting the burden of proving fault or negligence to the business operators; and
2. the Civil and Commercial Code, particularly in the context of tort law, may also be applicable in a broader sense for liabilities arising from

software or computer systems i.e., covering liability outside of consumer cases.

5. 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) ("Computer Crime Act"). This act specifically penalizes activities such as unauthorized access to computer data (hacking), phishing, and the misuse of software as a tool to cause harm or damage to another person or their property.

6. 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 customer in Thailand. The Civil and Commercial Code generally governs the contractual relationship.

7. 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. Given that the majority of software is provided by a foreign software house, the cap would typically follow the standard terms of such software house.

8. 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.

Given that a majority of software is provided by foreign software house, the cap would typically follow the standard terms of such software house. The above listed areas of liability would normally be subject to negotiation as to whether the liability would be subject to a cap at all, enhanced or a separate cap.

9. 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?

No, it is not a normal practice in Thailand.

10. 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.

11. 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.

12. 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.

13. Which body(ies), if any, is/are

responsible for the regulation of telecommunications networks and/or services?

The regulation of telecommunications networks and services in Thailand is primarily overseen by the National Broadcasting & Telecommunications Commission (NBTC).

14. 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 Organization 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 establishes licensing requirements for telecommunications business operators, which are classified into three types of telecom license: Type 1, Type 2, and Type 3. Each type has specific requirements, rules, and obligations that reflect the status and nature of the operator's business.

15. Which body(ies), if any, is/are responsible for data protection regulation?

The Office of the Personal Data Protection Committee (PDPC) is the responsible authority that oversees and ensures compliance with the Personal Data Protection Act (2019) (the "PDPA").

16. 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 the key piece of data protection law in Thailand, designed to safeguard personal data through the regulation of the collection, use, storage, disclosure, and processing of personal data. The PDPA sets out various obligations on entities and individuals handling personal data such as providing privacy notices, obtaining consent, and implementing appropriate security measures., etc. Failure to comply with the PDPA may result in three types of sanctions, which are civil penalty, criminal penalty, and administrative penalty.

17. 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 fine of THB 5 million for administrative penalties, whereas the maximum imprisonment period for criminal penalties is one year. However, civil penalties, including compensation for both actual and punitive damages, do not have a fixed maximum compensation amount as they vary depending on the specific circumstances of each case.

18. 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 the Data Processing Agreement (DPA).

19. 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"), introduced by the Office of National Digital Economy and Society Commission, was conducted in late 2022. The Royal Decree on AI is currently being reviewed by the Electronic Transactions Development Agency ("ETDA").

20. 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 impending Royal Decree on AI aims to regulate service businesses utilizing AI, adopting a risk-based approach and classifying AI systems into two distinctive categories: prohibited AI and high-risk AI, similar to the

approach in the EU. Prohibited AI means activities that aim to use AI to influence or alter human behaviour, resulting in potential bodily, mental harm or unfair discrimination that is disproportionate, such as AI employing subliminal techniques, social scoring, and real-time remote biometric identification systems in public spaces. On the other hand, high-risk AI includes AI-related activities 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 high-risk AI requires registration with the competent authority.

21. Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI?

No. Note that the Royal Decree on AI contains provisions relating to AI chatbots and deepfakes, requiring service providers and/or creators to inform the users of chatbot programs or viewers of deepfake content that they are interacting with AI or watching artificially created content, as the case may be.

22. Which body(ies), if any, is/are responsible for the regulation of blockchain and / or digital assets generally?

The Securities and Exchange Commission (the "SEC") is a responsible authority that regulates the offerings of digital tokens and businesses related digital assets, but there is no body regulating blockchain technology in general.

23. 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?

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 of the digital asset market and safeguard stakeholders, particularly investors in the market. For example, the token issuer must file a prospectus and obtain approval from the SEC prior to conducting ICOs. 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 services, (v) digital asset fund managers, (vi) initial coin offering portals, and (vii) digital asset custodial wallet providers.

24. Are blockchain based assets such as cryptocurrency or NFTs considered "property" capable of recovery (and other remedies) if misappropriated?

In terms of legal remedies, if misappropriation occurs and is carried out by or falls within the responsibility of digital asset operators, the SEC as the competent authority has the power to investigate and take appropriate actions, including the seizure or detention of properties related to the misappropriation of digital assets as deemed fit. It is important to note that the SEC takes a strict approach when dealing with cases involving the misuse of clients' digital assets by digital asset business operators and the custody and segregation of clients' assets.

25. Which body(ies), if any, is/are responsible for the regulation of search engines and marketplaces?

The ETDA serves as the supervisory authority of entities functioning as "digital platform service providers". In addition, the Office of the Consumer Protection Board (OCPB) regulates marketplaces in respect of their B2C e-commerce businesses, specifically those that operate online without a physical location for customers to physically inspect the products.

26. 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 that relate to search engines and marketplaces include the Electronic Transactions Act (2001), the Direct Sale and Direct Marketing Act (2002), the Royal Decree on Operation of Digital Platform Services Which Require Notification ("Royal Decree on Digital Platform"), and the Consumer Protection Act (1979).

The Electronic Transactions Act (2001) 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 on the enforceability and admissibility of electronic evidence in Thai legal proceedings.

The Direct Sale and Direct Marketing Act (2002) regulates "direct marketing activities", particularly those conducted through online channels, where customers can complete a purchase order on a platform without input from the platform operators e.g., carting systems. B2C e-commerce marketplace operators with these characteristics must obtain direct marketing registration with the OCPB under the Direct Sale and Direct Marketing Act. In addition, they are also required to comply with other compliance obligations such as preparing a return policy, submitting periodic reports, and maintaining a certain amount of business guarantees with the OCPB.

The Royal Decree on Digital Platform 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 residency or domicile of the digital platform service providers. Operators of such platforms are required to comply with certain obligations such as notifying the ETDA prior to commencing their business, preparing annual reports, disclosing terms and conditions, and appointing coordinators in Thailand.

27. Which body(ies), if any, is/are responsible for the regulation of social media?

The ETDA is a regulatory agency for social media platforms that function as digital platform service providers. In the context of computer-related offenses, the Ministry of Digital Economy and Society acts as the regulator.

28. Please summarise the principal laws (present or impending), if any, that govern social media, 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 Platform. The Computer Crime Act, which is the main law that governs social media in Thailand, aims to address various computer-related offenses. This includes offenses committed through social media platforms, such as spreading false information or sharing edited pictures of individuals with the intent to defame or humiliate the person depicted in the picture.

29. 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 – There are already several laws that regulate use and development of various types of AI in the pipeline.
2. Digital assets – It is likely that the relevant authorities will collaborate in levelling the playing field between (i) various types of digital assets and (ii) their corresponding traditional securities counterparts.
3. Digital platform – We expect that Thailand will have a more comprehensive and robust legal regime that governs digital platforms and websites.

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

No, the inclusion of provisions related to environmental commitments obligations under technology contracts in Thailand is rare. Nevertheless, the increasing awareness and importance of Environmental, Social, and Governance (ESG) considerations among Thai companies indicate a potential future trend, and it is expected that these provisions will become more prevalent in the near future.

Contributors

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

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

Nonthagorn Rojaunwong
Senior Associate
nonthagorn.r@mhm-global.com

Shaswat Weeramongkolkul
Associate
shaswat.w@mhm-global.com