Thailand


Kongkoch Yongsavasdikul


Teerachai Boonyaratgalin


Thamonwan Koosuwan

Kudun and Partners

1 E-Commerce Regulation

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

E-commerce entities are subject to various regulations, depending on the scope and nature of their business activities, including those related to the Electronic Transactions Act, B.E. 2544 (2001), the Commercial Registration Act (1956), the Direct Sale and Direct Marketing Act (2002) (the "**DSDMA**"), and the Royal Decree on Operation of Digital Platform Services Which Require Notification (2022) (the "**Decree on Digital Platform Service Business**") (which was recently issued on 22 December 2022 and will come into force and effect on 20 August 2023). In general, an e-commerce operator will be required to obtain commercial registration from the relevant commercial registration office under the Commercial Registration Act. The e-commerce operator may also be required to obtain direct marketing registration at the Office of the Consumer Protection Board ("**OCBC**") under the DSDMA if online trading can be conducted through online channels. In that case, the operator shall comply with the requirements under the DSDMA. Moreover, if an online platform business falls under the criteria of the Decree on Digital Platform Service Business, which governs digital platforms providing services as intermediaries between small business operators and consumers by using computer networks to offer goods, services, or intangible assets, including online marketplaces, social commerce, food delivery, space sharing, and online search engines, the operators of such platforms will be required to notify the Electronic Transactions Development Agency (the "**ETDA**") before conducting their businesses.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

The laws and regulations mentioned in question 1.1 are also applicable to B2C e-commerce businesses. In addition, the DSDMA, the Consumer Protection Act (1979), the Decree on Digital Platform Service Business and the Unfair Contract Terms Act (1997) are key regulations to enhance various aspects of consumer protection.

1.3 Please explain briefly how the EU's Digital Services Act and Digital Markets Act and/or equivalent local legislation, such as the UK's Online Safety Act and Digital Markets, Competition and Consumers Bill, may affect digital business in your jurisdiction.

There are currently no existing or anticipated regulations equivalent to the EU's Digital Services Act, Digital Markets Act, and/or equivalent local legislation, such as the UK's Online Safety Act and Digital Markets, Competition and Consumers Bill. However, Thailand has local pieces of legislation that share the same concepts as such Bills and Acts.

Business owners, companies, or any individuals ("**Entrepreneurs**") who wish to engage with customers via an online platform (such as websites that have the option to purchase and sell goods or services by electronic media via the internet, internet service providers, web hosting, and e-market places (a central market for buying and selling products, goods or services by electronic media via the internet)) must proceed with e-commerce registration with the Department of Business Development (the "**DBD**") and the ETDA.

Under the Business Registration Act, B.E. 2499 (1956) and the Ministry of Commerce Regulations on Persons who have Duties for Commercial Registration (No. 11), B.E. 2553 (2010), Entrepreneurs who engage in online platforms are required to apply for e-commerce registration. Furthermore, the ETDA requires that any Entrepreneurs who meet the criteria of the Electronic Transactions Act and the Decree on Digital Platform Service Business must register with the ETDA.

The rationale and advantages behind these pieces of legislation are: (i) to improve the reliability and confirm the existence of Entrepreneurs; (ii) Entrepreneurs can apply for a "Verified Trustmark" from the DBD that confirms that the Entrepreneur has met electronic business standard criteria; and (iii) Entrepreneurs who have acquired e-commerce registration are eligible to participate in training courses organised by the DBD.

Any Entrepreneurs who engage in online platforms and meet ETDA and DBD criteria without registration with the ETDA or DBD are considered to be in violation of the law and regulations and shall be subject to daily fine until such violation is corrected.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

The Personal Data Protection Act (2019) (the "**PDPA**") is Thailand's first consolidated law that governs personal data protection. The PDPA requires all organisations to implement measures concerning the collection, use, and/or disclosure of personal data by a personal data controller or processor, and to uphold all rights concerning personal data.

The enforcement of the PDPA has been fully implemented since 1 June 2022. The PDPA contains numerous principles for personal data protection, and the Personal Data Protection Committee (the "**PDPC**") has set out subordinate regulations specifying practices that business operators can implement in their business operations.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

The PDPA provides a number of requirements in relation to the collection, use, and disclosure of personal data, and thereby imposes certain restrictions on organisations' use and disclosure of personal data, as well as the requirement for the data subject to be notified in the event of any data leakage or breach.

To comply with the PDPA, organisations will have to identify the type of personal data they wish to use – general personal data or sensitive data – and will have to identify lawful bases for processing such data. The lawful bases on which to process general personal data are: consent; contract; legal obligation; legitimate interests; public task; vital interests; and archives for public interest or research or statistics. The lawful bases to process sensitive data are: explicit consent; legal claims or judicial acts; vital interests; legitimate activities by non-profit bodies, where they are made public by the data subjects; and legal obligations for specific purposes.

For instance, personal data obtained by the use of AI machines is considered biometric data, which is sensitive data under the PDPA. The PDPA describes biometric data as "personal data arising from specific technical processing relating to the physical or behavioural characteristics of a natural person, which allow or confirm the unique identification of a natural person, such as facial recognition data, iris recognition, or fingerprint recognition data". Therefore, when processing biometric data, data controllers or processors must obtain explicit consent from data subjects, except when processing health data, which can be done by relying on other lawful bases.

Digital health includes mobile health applications, electronic health records ("**EHRs**"), electronic medical records ("**EMRs**"), wearable devices, telehealth, telemedicine, and personalised medicine. These applications, records, and devices collect health data of data subjects. Since healthcare-related personal data is considered "sensitive data" under the PDPA, data controllers or processors who use digital health must obtain explicit consent from data subjects, except when the processing of healthcare-related personal data can be done by relying on other lawful bases.

Moreover, when FinTech or retail organisations or business operators process personal data for direct marketing, such organisations must rely on explicit consent as a lawful basis for processing personal data under the PDPA. Explicit consent must be obtained from data subjects because direct marketing is very invasive of their privacy, and organisations cannot thus expect such direct contact without first requesting data subjects' consent.

Organisations must ensure the implantation of appropriate and adequate organisational and technical security measures for personal data protection. The regulators, such as the Bank of Thailand (the "**BOT**") and the Securities and Exchange Commission of Thailand (the "**SEC**"), will also monitor business operators to ensure that they fulfil their responsibilities as regulated businesses in Thailand. The PDPA and the PDPC Notification re: Security Measures B.E. 2565 (2022) set out criteria on security measures, including organisational, technical, and physical measures that organisations can implement, such as access control, user access management, user responsibilities, audit trails, and personnel training.

2.3 What support are the government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

The PDPC, as the privacy regulator, is in the process of drafting and establishing the subordinate regulations under the PDPA, while the Digital Economy Promotion Agency ("**DEPA**"), the National Innovation Agency ("**NIA**"), and ETDA are the major regulators that drive support for and promote AI-related businesses and encourage the digital industry in Thailand to adopt new technologies. In addition, the BOT has developed key infrastructures to support upcoming digital products from FinTech sectors by collaborating with private or government sectors to work towards digital transformation. As FinTech startups are gradually playing an increasingly important role in the financial industry and the Thai economy, the Thai government is offering support to and regulating FinTech startups to increase access to financial services, improve efficiency and stimulate competition, as well as create innovation in the financial system. On the other hand, the SEC, which is the regulator for digital asset businesses, is also developing its standard measures to ensure that all licensed business operators improve their IT standard systems and infrastructure to keep up with the rapid changes in AI technology, in line with the ultimate goal of the SEC to protect public users.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The framework for policies and measures for the security of information technology systems is governed by the National Cybersecurity Committee (the "**NCS**") under the Cybersecurity Act (2019). The Cybersecurity Act specifically prescribes the prevention of cyber threats, and provides minimum standards for cybersecurity of organisations in both private and public sectors and important measures to cope with the risk of cyber threats from both inside and outside Thailand. The NCS has the authority to monitor and supervise compliance under the Cybersecurity Act.

In addition to the Cybersecurity Act, the Royal Decree on Cyber Crime Prevention and Suppression (2023) has also been recently updated. This regulation aims to protect consumers from internet scams and solicitations, particularly when their behaviour on e-commerce platforms exposes them to the risk of identity theft or fraud, resulting in money being stolen from bank accounts. The Royal Decree on Cyber Crime Prevention

and Suppression serves as a tool for the relevant authority to collaborate with all financial institutions to freeze bank accounts suspected of being used for fraudulent activities and integrate the use of AI technology to investigate suspicious transactions. Nevertheless, e-commerce businesses that wish to facilitate their customers by providing payment gateways need to obtain a payment licence from the BOT before receiving payments from their customers, and one of the requirements for the service provider is adequate IT security measures that shall comply with the BOT's standards. Please see our response in question 11.1 for more detailed information.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction. If there is any, how is that enforced?

The major regulations that apply to cybersecurity are:

1. The Criminal Code.
2. The Computer Crime Act (2017).
3. The Cybersecurity Act.
4. The PDPA.
5. The Royal Decree on Cyber Crime Prevention and Suppression.
6. The Electronic Transactions Act.
7. The Financial Institutions Businesses Act (2008) ("**FIBA**").
8. The Telecommunications Business Act (2001) ("**TBA**").
9. The Payment Systems Act (2017) (the "**Payment Systems Act**").
10. The Emergency Decree on Digital Asset Business (2018).

These laws are applicable and enforceable to all relevant persons specified thereunder.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

Driven by the growth of digital technologies and internet connectivity, e-commerce has been widely embraced by Thai consumers, and its popularity has increased rapidly in Thailand. In addition to being the second-largest e-commerce market in ASEAN, research shows that e-commerce in Thailand will continue to expand by approximately 20% each year during the next five years.

With the introduction of social distancing and lockdown regulations during the recent COVID-19 pandemic, which restricted consumers from visiting physical stores, this became an important factor in influencing consumers' move towards e-commerce and cashless payment even further, due to the convenience thereof. This new trend incorporates AI technology, particularly big data management, and highlights how technology will be a significant factor in mapping consumer habits in the next decade.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery-type culture?

In alignment with global trends and as part of the Thailand 4.0 policy, the Thai government has been encouraging the culture of a cashless society and the use of e-payment through various methods, including, most recently, governmental measures, such as, the Rao Chana programme (We Win), a financial aid scheme to an additional 2.4 million people that provides cash incentives to new users, and the Khon La Khrueng programme (Let's Go Halves), a co-payment scheme to encourage cashless payments in the food and travel industries whereby the government will pay half of the price of food or accommodation for travellers, through business owners who registered with the programme via digital wallet. These two campaigns were products of changes in technology that resulted in new consumer behaviour trends that regulators were forced to keep up with in order to stay abreast of market conditions.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

There is no evidence that Thailand-based websites perform better in jurisdictions other than Thailand.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Like any other e-commerce firms doing business in other jurisdictions, the local languages of the relevant targeted markets and consumers are used when selling products or services in such other jurisdictions. However, it is typical for e-commerce firms in Thailand to apply a bilingual approach (Thai and English) in marketing to overseas customers. Recently, AI technology has played an important role in facilitating translation tasks for business operators, which resulted in reducing the translation gap between local and foreign markets.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

Thai consumers prefer web-interface design concepts that are user-friendly, quick and responsive with readily available filters and diverse payment methods. They also value the presence of security systems on the interface, which prevent identity theft and have prevented billions of criminal activities in recent years.

4.6 Has the COVID-19 pandemic had any lasting impact on these cultural norms?

The COVID-19 pandemic has accelerated and shifted consumers' shopping habits towards e-commerce, e-payments, as well as raised awareness of the work-from-home working style. This has resulted in a significant market change in Thailand.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

The Department of Intellectual Property (the "DIP") is the regulatory authority responsible for IP-related matters in Thailand. For online IP rights enforcement, in the case that goods that are infringing on another person's IP rights are being sold

on e-commerce platforms, clear evidence of infringement as well as the name of the infringing seller, prices of infringing goods and products, and the location of the infringing goods and products should be collected. The next step is that the owner of the IP rights should inform the e-commerce platform about the person who is counterfeiting or imitating the IP rights so that the platform operator can then order them to stop the sale of those infringing goods and products on the platform.

Under Thai law, any person who counterfeits a trademark, service mark, certification mark or collective mark registered in Thailand by another person shall be liable to imprisonment for a term not exceeding four years or a fine not exceeding THB 400,000 or both.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

In the event that the owner of the IP rights requests an e-commerce platform to serve the notice mentioned in question 5.1 to the person who committed the infringement, it is common that the e-marketplace website service provider would request the owner of the IP rights to present the registration certificate issued by the DIP as evidence of ownership before serving the notice to the person who committed the infringement. Therefore, the owner of the IP rights should ensure that the registration certificate is in place, valid and ready as it may be requested by the e-marketplace website service provider.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

Cloud service providers and third party-owned data centres are considered data processors under the PDPA. Therefore, any entities that contract with third party-owned data centres and cloud service providers shall enter into a data processing agreement (the "**DPA**"), which outlines the scope and purposes of the data processing. In the absence of the DPA, such entities should check the terms and conditions to establish whether the scope and purposes of the processing have been addressed.

The use of cloud service providers and data centres located in other countries, where only the data controller, data processor, and their personnel have access to such personal data in the cloud storage, is not considered a transfer of personal data to foreign countries pursuant to the PDPC Notification re: Criteria for Providing Protection to Personal Data Transmitted or Transferred to Foreign Countries Under Section 28 of the PDPA B.E. 2566 (2023) and the PDPC Notification re: Criteria for Providing Protection to Personal Data Transmitted or Transferred to Foreign Countries Under Section 29 of the PDPA B.E. 2566 (2023) (the "**PDPC Notifications re Cross-Border Transfer**"). If other parties other than the data controller, data processor, and their personnel have access, they must transfer personal data in compliance with the PDPC Notifications re Cross-Border Transfer.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Pursuant to the Notification of the NBTC Prescribing Type and Category of Telecommunication Business Requiring the Telecommunication Business License, a service provider for a data centre needs to obtain the licence from the Office of the National Broadcasting and Telecommunications Commission ("**NBTC**") before operating the business in Thailand. As previously discussed, servers/data centres located in Thailand are considered data processors under the PDPA. Consequently, the DPA between the data controllers and such servers/data centres must be entered into. However, there are no issues regarding cross-border transfer when transferring personal data to such servers/data centres.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your jurisdiction?

No specific technologies have been adopted by private enterprises and government border agencies to digitalise international trade.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forward?

Thailand's adaptation of digital technologies requires collaboration between both public and private sectors, and it should start with the government sector incentivising the users and encouraging the digitalisation of all transactions in order for the users to absorb technology into their daily lives. Since Thailand has been using analogue technology for such a long time, there is a huge opportunity to move forward into the digital age, but it needs full support from the government.

8 Tax Treatment for Digital Businesses

8.1 Please give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction. These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Recently, the Thailand Board of Investment (the "**BOI**") amended its promoted business activities under the Investment Promotion Act (1979) by repealing the promotion of software (category 5.7), e-commerce (category 5.8), and digital services (category 5.9) and adding a new category involving the development of software, platform for digital services, and digital content activities (category 5.10). The privileges under these new BOI promoted businesses include, among others, an eight-year corporate income tax ("**CIT**") exemption and a machine import duty exemption. To qualify for these BOI's privileges, business owners must fulfil certain requirements and conditions, as prescribed by the Investment Promotion Act and its related regulations.

Another recent enactment pertaining to tax reliefs for digital assets business and related transactions was introduced through Royal Decree No. 779, issued under the Revenue Code (1938) (and amendments). Intending to stimulate and enhance competitiveness in Thailand's digital asset market, this Royal Decree stipulated the exemptions of CIT and Value-Added Tax ("**VAT**") for qualified transfers of investment tokens in both the primary and secondary markets.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

The SEC and the Revenue Department of Thailand have expanded the scope of personal income tax to cover digital assets; namely, cryptocurrency and digital tokens and any other revenue gained from conducting business involving digital assets. Any person who makes capital gains from digital assets must pay withholding tax on the profit they received on the trade and the cumulative capital gains for each calendar year. If they receive any incentives from the tokens (such as investment tokens or utility tokens), such person needs to report this to the Revenue Department and pay 15% personal income tax on such amount. This could be considered a double tax payment that may be a barrier for investors and token developers and jeopardise Thailand's position as being a country that supports digital asset businesses. Nevertheless, as this has only recently been announced, the guidelines for this tax deduction are not rigid in practice and, despite opposition from taxpayers, they are currently being enforced and further updates will be announced by the tax authority.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please describe the advantages and disadvantages of the available employment status models.

The Thai government has been encouraging all companies to support their employees by using technology solutions, as seen during the COVID-19 pandemic era, especially in terms of communication, when information technology played an important role in enabling companies to continue functioning. It has accelerated the learning curve process for all private and public sectors to comply with technology such as e-filing and cloud services for data warehouses and online meetings. This has led to the mandated notification of government officials changing from hard copies to soft copies and storing them in the cloud system. This mandatory measure also helps to facilitate people when they contact officials, since they can access a big data warehouse that is protected by the Cybersecurity Act. However, it means that a huge number of government officials may face technology disruption and layoffs, and their empty positions may be replaced by AI technology.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There is no specific regulation to support remote working from companies' offices in Thailand. However, Thailand's government previously encouraged all companies to allow their employees to work from home to prevent the spread of COVID-19, and some companies still implement their work-from-home policies today. This shows that technology could reduce some unnecessary costs, such as office rent and transportation fees, and signifies the return of the work-life balance for some employees who can now spend time at home with their family or pets.

9.3 What long-term effects or changes are likely to result from the COVID-19 pandemic?

Thailand has embraced the work-from-home culture and encouraged the whole country to adopt online meetings and online payments. This adaptation can be seen in the growth of online shopping and new e-commerce businesses established to serve the demands of cultural change. It also reflects a shift in interior design culture to include the home office and any working station that supports physical health and lifestyle tailored to working from home.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

The movement of Thai markets towards digital business has accelerated rapidly and as a result, improvements to the existing legal and regulatory frameworks governing e-payments should and are required to be improved, or tax relief programmes should be provided concurrently with the expansion.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

Apart from our answer in question 4.2, there is no direct regulation that provides any incentive for digital businesses, but the BOI has nonetheless extended their promoted business activities to cover more digital business activities that qualify for tax incentives in Thailand as mentioned in question 8.1.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The Thai government is currently focusing on improvement of the logistics and warehouse sectors, facilitating and supporting e-payment systems, and expanding online retail markets throughout the region. On the other hand, the Thai government also issued the Royal Decree on Cyber Crime Prevention and Suppression to combat identity theft in Thailand, which is often on a large scale, such as scams involving call centres.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

The Payment Systems Act was introduced to regulate all payment-related businesses that might have an impact on the public sector. Service providers of certain regulated payment services need to register or obtain a licence to conduct payment service businesses in Thailand, whereby depending on whether it is for a card issuer, e-money, or e-payment service such as acquirer, payment facilitator, and payment on behalf of others.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

Please see our answer to question 11.1. For e-payment service

providers regulated by the BOT, the penalty for not complying with the notice requirement is a fine of between THB 1 million and THB 2 million, depending on the type of e-payment service provider.

12 Digital and the Green Economy

12.1 With the current global emphasis on the environment and sustainability, is there any current or anticipated legislation in that area that is likely to impact digital business in your jurisdiction?

There are currently no existing or anticipated regulations that may impact digital businesses in Thailand.

12.2 Are there any incentives for digital businesses to become 'greener'?

There are currently no regulations to encourage digital businesses to become more environmentally friendly.

12.3 What do you see as the environmental and sustainability challenges facing digital businesses?

Digital businesses consume a considerable amount of energy, which is a major concern in terms of global warming and natural disasters. Hence, this is not merely an issue that affects one jurisdiction but is actually a global issue. Protecting the planet should be a joint effort. All countries should work towards this by introducing relevant and effective regulations to support greener business, especially digital businesses.

Kongkoch Yongsavasdikul's principal areas of practice include corporate, mergers & acquisitions, project financing, fundraising, capital markets, including initial public listing (IPO), corporate restructuring, and infrastructure funds. He has spent around 15 years in practice representing both the buy and sell side in a wide spectrum of public and private transactions, including entire business transfers (EBT) of companies across a broad range of industries such as financial services, digital asset exchange platforms, healthcare, renewable energy (solar and wind), real estate and TMT, including tech startups and e-commerce. His capital markets credentials include establishing some of the award-winning and ground-breaking infrastructure funds in the country.

Kudun and Partners
34/3 Vivre Langsuan, 4th, 5th, and 6th Floors
Soi Langsuan, Lumpini, Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 838 1750
Email: kongkoch.y@kap.co.th
LinkedIn: www.linkedin.com/in/kongkoch-yongsavasdikul-497316189

Teerachai Boonyaratgalin is an associate with Kudun and Partners. He is a corporate lawyer with a particular focus on digital law. He has assisted both domestic and international clients across multiple areas of law, including corporate and commercial, FinTech and digital asset law, and dispute resolution.

Kudun and Partners
34/3 Vivre Langsuan, 4th, 5th, and 6th Floors
Soi Langsuan, Lumpini, Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 838 1750
Email: teerachai.b@kap.co.th
LinkedIn: www.linkedin.com/in/teerachai-boon

Thamonwan Koosuwan is an associate with Kudun and Partners. She is a corporate lawyer who is well versed in advising both domestic and international clients with a particular focus on digital law. Her expertise extends across multiple areas of law, including corporate and commercial, FinTech and digital asset law.

Kudun and Partners
34/3 Vivre Langsuan, 4th, 5th, and 6th Floors
Soi Langsuan, Lumpini, Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 838 1750
Email: thamonwan.k@kap.co.th
LinkedIn: www.linkedin.com/in/thamonwan-koosuwan-9b60621ba

Kudun & Partners was founded in 2015, born from a desire to practise law with a dynamism and creativity that simply was not available anywhere else. Since then, we have attracted domestic and international recognition from top legal publications, worked with some of the world's largest companies and advised on multi-million-dollar transactions. Our firm's singular outlook continues to set us apart and enables us to meet and exceed clients' commercial objectives.

Digital law practice

Our digital law practice consists of some of the most prolific digital law-savvy lawyers in Thailand, offering a broad range of legal advisory services and quality solutions to both local and international clients across a broad scope of legal matters for a wide range of TMT industries. We understand the challenges and rewards of staying innovative and profitable amid fast-paced change in the information technology and communications industry.

Our firm has been providing legal advice on both contentious and non-contentious issues on a spectrum of practice areas to some of our largest TMT clients. We are trusted to provide legal advice on heated digital asset-related matters and represent clients who are significant in the digital asset market.

Experience across a wide range of issues

We advise clients on digital business-related legal issues, including:

- Regulatory advice.
- Systems procurement and integration.
- Legal compliance, including data privacy and protection, information security and record retention.
- Cybersecurity framework.
- E-commerce regulations for domestic and foreign providers.
- E-payment/online payment gateway.
- Broadcasting/satellite and digital agreements.
- Data centres and cloud storage.
- TMT dispute and negotiation, including litigation, arbitration and mediation.
- Employment law implications for agile workforce.
- Tax planning, including transfer pricing and both direct and indirect taxation for digital businesses.

www.kap.co.th

KUDUN & PARTNERS