

Thailand: 2026 AI Regulatory Landscape for Businesses

Regulatory insights and compliance considerations for responsible AI adoption

In brief

Thailand's AI regulatory landscape is evolving. A comprehensive national AI framework is under development and is expected to progress toward enactment within the next few years. It introduces a risk-based model, duties for high-risk AI providers and deployers, individual rights, and oversight by the forthcoming AI Governance Center.

In parallel, multiple sector-specific rules in areas such as judicial processes, consumer protection, and financial services have been issued. Numerous non-binding guidelines shape expectations on ethical and responsible AI use. Recently, a draft on AI and privacy was released for public hearing.

Businesses therefore face a hybrid regulatory environment and should proactively enhance AI governance through internal policies, updated external-facing documents, and clear documentation, both to prepare for stricter transparency and accountability requirements and to mitigate legal risks under existing laws.

Contents

[Key takeaways](#)

[In more detail](#)

[Comprehensive AI legislation – Draft framework under development](#)

[Sector-specific AI regulations](#)

[Non-binding AI guidelines](#)

[Key considerations for businesses](#)

[Contact Us](#)

Key takeaways

1. Thailand is moving toward a comprehensive national AI law

A new AI framework with duties for high-risk AI providers and deployers is under refinement and expected to advance toward enactment in the next few years. Businesses should anticipate future obligations around transparency, accountability, and human oversight.

2. Sector-specific AI rules already impose real compliance duties

Courts, financial regulators, and consumer protection authorities have issued binding and quasi-binding requirements. Examples include mandatory AI-disclosure for court filings, AI-generated advertising labels, and the Bank of Thailand's AI risk-management expectations.

3. Non-binding guidelines are shaping regulatory expectations

Numerous government bodies now publish AI ethics, governance, security, and sector-specific guidelines. These increasingly influence enforcement trends and set the baseline for responsible AI practices. Companies should ensure that their practices align with the expectations of their respective regulators.

4. Businesses face immediate exposure under existing laws

Without a unified AI statute, companies must still manage legal risks under intellectual property laws, personal data protection laws, consumer protection laws, cybersecurity laws, the computer crime law, and various sector-specific regulations.

5. Companies should proactively strengthen AI governance now

Companies should consider establishing a formal AI governance model and internal AI usage policies. Existing practices and documentation should be reassessed to ensure they are fit for purpose in light of increasing regulatory scrutiny.

In more detail

Over the past few years, Thailand has seen significant and accelerating developments in the governance of artificial intelligence (AI).

To provide a clear and structured overview of these changes, this newsletter highlights key updates across four areas: (i) Thailand's progress toward a comprehensive national AI framework, including the Draft Principles of Artificial Intelligence Law currently under refinement; (ii) the emergence of sector-specific AI regulations that vary in binding effect and enforcement; (iii) the growing body of non-binding AI guidelines shaping expectations around responsible AI use; and (iv) practical implications and compliance considerations for businesses operating amid this rapidly evolving regulatory environment.

Comprehensive AI legislation – Draft framework under development

The centerpiece of Thailand's future AI regime is the Draft Principles of Artificial Intelligence Law ("**Draft AI Principles**"), released for public consultation in mid-2025 and now undergoing refinement by the Electronic Transactions Development Agency (ETDA). The Draft AI Principles are expected to progress toward enactment within the next two to three years.

The general principles set out under the Draft Principles are derived from the UNCITRAL Model Law and are intended to support user confidence in deploying AI. This includes: (i) non-discrimination; (ii) AI as a tool; and (iii) exception for unexpected actions.

Key principles of the Draft AI Principles

Principles	Description
1. Designation of prohibited and high-risk AI	<ul style="list-style-type: none">The Draft AI Principles adopt a risk based model by empowering "central agencies" (e.g., the AI Governance Center (AIGC) under the ETDA) and "sectoral regulators" (e.g., the Bank of Thailand (BOT) and Office of Insurance Commission (OIC)) to define lists of "Prohibited" and "High-Risk" AI.
2. Establishment of duties for high-risk AI providers	<ul style="list-style-type: none">Risk management: High-risk AI providers must implement risk management systems in accordance with international standards (e.g., ISO/IEC42001:2023, or NIST Risk Management Framework). Central agencies and sectoral regulators are empowered to specify further details in the subordinate legislation.Legal representative: Offshore providers of high-risk AI systems are required to appoint a local legal representative in Thailand.Serious incident: High-risk AI providers must report serious incidents to the central agencies.
3. Establishment of duties for high-risk AI deployers	<ul style="list-style-type: none">High-risk AI deployers must have personnel to oversee AI operations, maintain logs of the AI system's operations for an appropriate period, ensure the quality of data if the deployer developed the system using their own datasets, notify affected individuals if the use of a high-risk AI could negatively affect their life, physical well-being, or fundamental rights, and cooperate with regulatory authorities in investigating AI deployments that have resulted in errors or damage.
4. Duty of care approach	<ul style="list-style-type: none">The Draft AI Principles adopt a duty of care approach for high-risk providers and deployers (e.g., if an AI provider can demonstrate that they have fulfilled their duty of care, they will not be held liable. However, if an AI provider fails to meet this duty and damages occur, it could be held liable.)
5. Regulator	<ul style="list-style-type: none">The responsible institution will be the AIGC. Its tasks include providing consultation to organizations on AI implementation, supporting testing projects and sandboxes, compiling statistical data on AI readiness, and developing collaborative networks both domestically and internationally.

<p>6. Rights of the affected person from the decision of high-risk AI</p>	<ul style="list-style-type: none"> • Right to be notified: Persons must be notified that AI will be used in their cases. • Right to be explained: Persons must be provided with sufficient explanations to understand the role of artificial intelligence in the decision-making process and the key factors used in making decisions. • Right to appeal: Persons have the right to request that decisions must be made by the business operator without the use of AI.
<p>7. Penalty</p>	<ul style="list-style-type: none"> • Criminal penalties: In cases where AI is used to create images, sounds, or videos that constitute sexual content or false statements related to an election. • Administrative fines: In cases of providing or deploying prohibited-risk AI. • Others: For high-risk AI, it remains uncertain whether the duties of high-risk AI providers and deployers will be imposed as mandatory requirements subject to administrative fines, or alternatively treated as voluntary obligations, where compliance may give rise to favorable presumptions for injured parties in tort claims, while non-compliance may result in the loss of eligibility to access supportive measures.

Additionally, other principles were proposed in the Draft AI Principles, including:

- Supportive mechanisms in finance and tax, infrastructure, R&D, text and data mining, sandboxes, and human resources.
- Misalignment measures, including labeling requirements for AI-generated content and potential additional obligations for generative AI.
- Legal enforcement processes, including orders requiring AI providers or deployers to terminate the provision or deployment of AI, orders requiring platform business operators to terminate the hosting of AI, and restrictions on Thai users' access to AI.

Once adopted, the Draft AI Principles will supersede earlier draft instruments, including: (i) the Draft Royal Decree on Business Operations that Use Artificial Intelligence Systems; (ii) the Draft Act on the Promotion and Support for National AI Innovations; and (iii) its draft subordinate regulations (i.e., the ETDA's draft risk management and sandbox notifications).

Sector-specific AI regulations

Although comprehensive AI legislation is still pending, Thailand has issued sector-specific regulations governing AI related activities, the legal binding effect of which depends on various factors such as the nature of the provisions, the issuing entity's citation of law as a source of legal authority, and the sectoral regulator's enforcement practices and interpretations.

The key sectoral regulations in Thailand include:

- **AI in the practice of law: Judicial guidance and rules governing the use of AI in court proceedings**
 - **Guidance by the President of the Supreme Court re: Use of Artificial Intelligence in Performance of Judicial Case Work B.E. 2568 (2025)** – Recommendations and requirements on the use of AI in the judicial system by judges and court officials emphasize key principles in performing judicial functions and AI ethics, such as the judge's fairness and absence of bias, official secrecy, data protection, utmost accountability for the integrity of the justice system, and technological safety and trustworthiness.

For example, judges using AI in proceedings must still uphold their judicial independence when exercising discretion in deciding a case, without being directed or interfered with by AI technology, bearing in mind the limitations stemming from associated risks, such as algorithmic bias.

- **Civil Court's Directive on Using Artificial Intelligence Technologies for Preparing Pleadings or Other Documents in the Court Filings B.E. 2568 (2025)** – A legally binding directive mandating lawyers and parties in court cases within the jurisdiction of the Civil Court to comply with AI-generated court filing rules, which include ensuring the accuracy of facts, legal citations and evidence used in pleadings or any other documents; labelling any pleadings and other documents that rely on AI, whether in part or in full, with mandatory disclosure wordings such as, "[the following content is created with artificial intelligence technology]"; and providing a representation on the accuracy of the AI-assisted pleadings and other documents to be filed to the Civil Court, among others.
- **Guidelines by other local courts of first instance** – For the past few years, we have also seen an interesting judicial trend where some lower level courts issued certain guidelines on the use of AI technology in the proceedings within their jurisdiction. For example, Maha Sarakham Court Notification re: Direction for Practice Relating to Using the Artificial Intelligence Technology for Preparation of Case-related Documents for Court Filings B.E. 2569 (2026). This demonstrates attempts by Thailand's judiciary branch to keep pace with technological advancements.

- **AI disclosure in advertisements under Consumer Protection Law**

On 18 July 2025, the Office of Consumer Protection Board (OCPB) issued a notification governing the use of AI in generating advertising content, addressing the concerns about misleading or exaggerated advertising claims. Particularly, if any advertising content is generated by AI, the notification provides that the business operator or advertiser discloses the use of such AI by labelling the content with a clear statement accordingly (e.g., "image was created by AI").

- **AI risk management in the financial services sector**

On 12 September 2025, the BOT issued a document titled "Policy Direction of the Bank of Thailand re: Risk Management of the Use of Artificial Intelligence System" ("**BOT AI Policy Direction**" or "**Direction**"). The document is intended for BOT-regulated financial service providers (e.g., financial institutions and payment service providers under the BOT's supervision) to use as a framework for managing risks arising from the use of AI systems in a manner appropriate to the nature of such use, aligning with the principle of "responsible AI" use. Importantly, this BOT AI Policy Direction serves as an additional piece of policy direction to the BOT's previously established rules, guidelines and policy directions, such as the Information Technology Risk rules, the IT Risk Management Implementation Guideline, the Third Party Risk Management Implementation Guideline, the Data Governance policy direction, and the Market Conduct Rules. Although formally framed as a guideline-like instrument, BOT-regulated entities are expected to adhere to its requirements in practice.

In essence, this Direction classifies the risks arising from AI systems into 3 main non-exhaustive types: (1) Data Risk; (2) Model Development Risk; and (3) Cyber Threat Risk, while establishing the principles of AI risk management in line with the generally accepted "responsible AI" principle (e.g., "FEAT" principle – fairness, ethics, accountability and transparency) and setting out the implementation plan for AI risk management covering AI governance and AI development and security.

Non-binding AI guidelines

Complementing binding rules, Thailand has several influential soft law instruments promoting ethical, transparent, and secure AI development and use. Key sectoral nonbinding guidelines in Thailand include:

Industry / Sector	Key AI Guidelines
1. General	<ul style="list-style-type: none"> ● Digital Thailand AI Ethics Guideline issued by the Ministry of Digital Economy and Society (MDES) ● Thailand AI Ethics Guideline issued by the MDES ● Thailand Artificial Intelligence Guidelines 1.0 issued by Chulalongkorn University

	<ul style="list-style-type: none"> • Thailand AI Governance Guideline for Executives issued by the Electronic Transactions Development Agency (ETDA) • Generative AI Governance Guideline for Organizations issued by the ETDA • ETDA's study results and policy recommendations on advancing Thailand's AI adoption in line with UNESCO's Recommendation on the Ethics of AI issued by the ETDA
2. Insurance	<ul style="list-style-type: none"> • AI Governance Guideline issued by the OIC. Applies to the insurance sector, establishing a risk based framework for managing emerging AI risks.
3. Data Protection (Recent development)	<ul style="list-style-type: none"> • Draft of Guidelines on Personal Data Protection in the Development and Use of AI issued by the Office of the Personal Data Protection Committee. Applies to public and private organizations that are deemed data controllers and data processors under the Personal Data Protection Act.
4. Stock Exchange and Capital Market	<ul style="list-style-type: none"> • Regulatory Framework for the Use of AI and ML in the Capital Market issued by the Securities and Exchange Commission (SEC). Applies to service providers operating within capital markets to support responsible AI adoption.
5. Government Agencies	<ul style="list-style-type: none"> • AI Government Framework issued by the Digital Government Development Agency (DGA). Applies to government agencies. • AI for Government Administration and Services issued by the DGA. Applies to government agencies and is intended to guide the deployment of AI in government administration and services responsibly and effectively.
6. Science and Technology	<ul style="list-style-type: none"> • AI Ethics Guideline issued by the National Science and Technology Development Agency (NSTDA). Applies to personnel of the NSTDA, persons participating in research or receiving NSTDA research funding, private sector entities using the physical space in the Thailand Science Park (TSP) and the Eastern Economic Corridor of Innovation (EECi), including relevant subcontractors. The Guidelines set out principles for ethical research, development, application, and transfer of AI and data driven systems, balancing innovation with risk management. • AI Security Guideline issued by the National Cyber Security Agency (NCSA). Applies to internal and external stakeholders of an organization and societal stakeholders and regulatory bodies to support secure development, management, and use of AI, addressing risks such as cyberattacks, data leakage, and systemic manipulation, based on ISO/IEC, ENISA, OWASP and domestic regulations. • Several voluntary AI technical standards and guidelines issued by the Ministry of Industry (MOI). Applies to the industrial sector, promoting safe, responsible, and fair AI deployment
7. Media	<ul style="list-style-type: none"> • Guideline on the Ethical Use of Artificial Intelligence (AI) in the Journalism Profession B.E. 2567(2024) issued by the National Press Council of Thailand. Applies to media organizations, media professionals, newsroom staff, and supporters of media and news operations. The guideline sets out rules governing the use of AI in publishing news and information to the public.
8. Healthcare	<ul style="list-style-type: none"> • Guidelines for the Supervision of Software and Artificial Intelligence Used as Medical Devices issued by the Medical Device Control Division, Food and Drug Administration (FDA). Applies to manufacturers and importers of software and AI classified as medical devices. The guideline provides criteria for determining whether software or AI falls within the definition of a medical device subject to regulatory oversight. It also outlines risk classifications, advertising requirements, documentation for manufacturing and importation, and cybersecurity obligations.
9. Judicial	<ul style="list-style-type: none"> • Recommendations on the use of AI in judicial work issued by the President of the Supreme Court. Applies to judicial personnel affirming that AI may be used but only with judicial responsibility, confidentiality, independence, and the careful selection of suitable technologies.

Key considerations for businesses

Key legal exposures under existing laws

In the absence of a unified AI statute, companies must manage regulatory exposure under existing legal frameworks, especially:

- **Intellectual Property laws** – especially where AI involves copyrighted input or generates potentially infringing outputs.
- **Personal Data Protection Act** – covering legal basis for processing, data-processing agreements, and the handling of training and input data.
- **Consumer Protection Act** – including risks related to misleading advertising and AI generated promotional content.
- **Cybersecurity obligations** – including incident-response requirements and secure-development practices.
- **Computer Crime Act and Criminal Code** – when AI generates illegal content such as lèse-majesté, fraudulent, pornography, sexual harassment, and defamation content.
- **Sector-specific regulations** – such as those imposed on banking, insurance, and industrial sectors.

Practical steps for businesses

As AI adoption expands, regulators are stepping up scrutiny, particularly in high-risk use cases and consumer-facing applications, making it essential for businesses to proactively strengthen their AI governance and compliance readiness.

To prepare for the forthcoming AI law and mitigate current legal and operational risks from existing laws that already apply, businesses should consider:

1. Establishing an AI governance model

Define end-to-end processes for selecting AI products, identifying permitted use cases, conducting risk assessments, determining user roles and permissions, delivering training, setting human oversight and model-management requirements, establishing approval workflows, establishing an AI committee to oversee and enforce the AI Governance Model, and defining criteria for moving from trial use to full deployment.

2. Implementing internal AI usage policies

Develop clear internal policies that specify the permitted and prohibited uses of AI, expectations for employee conduct, data handling requirements, penalties for employee misconduct, and escalation procedures.

3. Updating external -facing documents

Revise privacy notices, customer service terms and conditions, consent forms, vendor agreements, marketing and advertisement disclaimers, AI incident reporting channel, and disclosures to clarify AI usage.

4. Reviewing AI-related agreements

Conduct a structured review of AI-related contracts to identify key risks, listing allowed and prohibited AI use cases, including allocation of liability, indemnification obligations, data usage rights, model training permissions, performance warranties, and compliance responsibilities. Where appropriate, negotiate stronger contractual protections to ensure that risk is proportionately shared and that obligations reflect the operational realities and regulatory requirements applicable to AI deployment.

5. Maintaining documentation

Keep evidence of usage, log, risk assessments, human oversight mechanisms, and duty of care compliance to prepare for future regulatory requirements.

Call to action

With AI increasingly embedded in business operations and regulatory developments accelerating, companies should take steps now to ensure they remain prepared. Companies should begin aligning internal direction, reviewing their current AI use cases, and planning for more structured AI governance.

Proactive preparation, rather than reactive compliance, will place companies in a stronger position as new rules and sector-specific expectations continue to emerge, and Thailand's first comprehensive AI legislation is underway

Contact Us



Pattaraphan Paiboon
Partner
pattaraphan.paiboon
@bakermckenzie.com



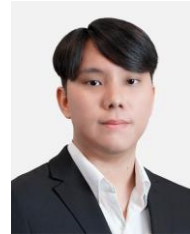
Kritiyanee Buranatrevedhya
Partner
kritiyanee.buranatrevedhya
@bakermckenzie.com



Aue-angkul Santirongyuth
Associate
aue-angkul.santirongyuth
@bakermckenzie.com



Pimpisa Ardborirak
Associate
pimpisa.ardborirak
@bakermckenzie.com



Pirun Suttiprapha
Associate
pirun.suttiprapha
@bakermckenzie.com

© 2026 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of the this Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.

