

Thailand: Draft AI Act - Seven Key Implications

Thailand's Draft AI Act introduces the country's first comprehensive AI regulation.

In brief

On 9 July 2026, the ETDA released the Draft AI Act for public consultation. If enacted, it would become Thailand's first comprehensive AI regulation.

- **Broad application.** Applies to developers, providers, deployers, and platform operators, including offshore entities.
- **Risk-based approach.** AI systems are categorized into prohibited AI, high-risk AI, AI subject to licensing requirements, and AI subject to transparency obligations (Deepfakes, chatbots and Gen-AI).
- **Data localization and controlled contracts.** Vendors serving government agencies and CII could be subject to mandatory contractual terms and data-localization requirements.
- **Strict liability and enforcement.** Strict and joint liability, alongside powers to suspend services and deployment, order recalls, and block AI systems in Thailand.

Stakeholders should participate in the public hearing, closing on 14 August 2026.

Contents

In more detail

Purpose and extraterritorial application
Innovation-friendly aspect: Self-regulation, trust-mark, and AI sandbox
Seven key business implications
Next steps
Contact us

In more detail

Purpose and extraterritorial application

The Draft Act on Artificial Intelligence B.E. ("**Draft AI Act**"), issued by the Electronic Transactions Development Agency (ETDA), aims to address risks associated with AI, including discrimination, privacy breaches, cybercrime, misinformation, and regulatory challenges.

The Draft AI Act has extraterritorial reach. It would apply not only to activities taking place in Thailand, but also to AI systems developed, provided, or deployed outside Thailand where they affect individuals in Thailand. Exemptions would apply to certain activities, including personal or household use, approved academic research, and pre-commercial research and development.

Innovation-friendly aspect: Self-regulation, trust-mark, and AI sandbox

The Draft AI Act includes several measures aimed at promoting AI innovation, including support for industry-led best practices and self-regulatory mechanisms, recognition of local and international standards, AI certification and trust-mark schemes, and an AI sandbox framework that allows businesses to test innovative AI solutions in a controlled environment. Together, these measures reflect an effort to balance AI governance with innovation and may provide opportunities for businesses to demonstrate responsible AI practices, engage with regulators, and build trust in AI-enabled products and services.

Seven key business implications

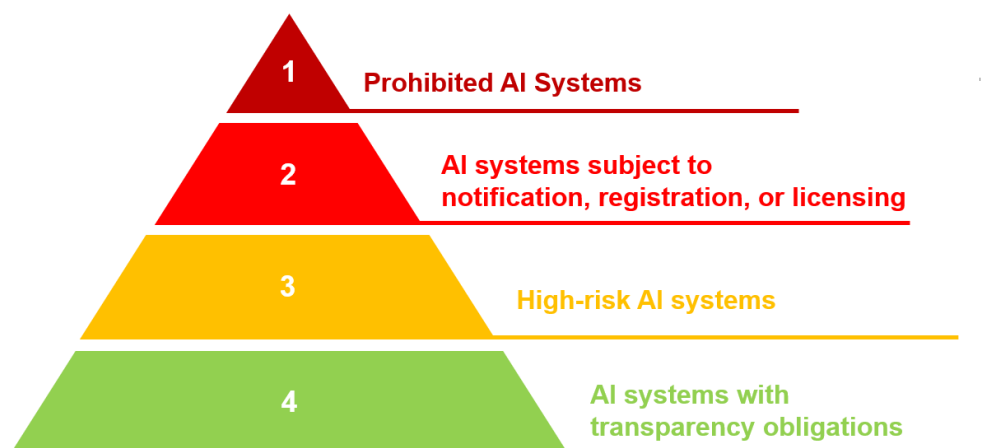
Set out below are seven key implications for business operators developing or deploying AI systems covered by the Draft AI Act.

1. Classification of AI systems - A risk-based approach

The Draft AI Act adopts a risk-based framework and would apply broadly across the AI value chain, including AI developers, providers, deployers, and platform operators. Rather than regulating all AI systems in the same way, compliance obligations would differ according to the level of risk associated with the AI system. The Draft AI Act would be

administered by the Minister of Digital Economy and Society and steered by the "Specialized Commission on Implementation of National Artificial Intelligence Plan" ("**Commission**").

Operators should assess the AI system and implement an appropriate compliance program. Please see the summary of the AI classification, obligations, and sanctions below.



Type	Regulated AI	Key obligations	Legal sanctions
1. Prohibited AI systems	The deployment of an AI system which impacts any of the following risks: - Subliminal techniques - Widespread unfair discrimination through the processing of large datasets - Other risks to be prescribed	The Draft AI Act prohibits the deployment of an AI system which impacts risks as prescribed.	Civil liability No prescribed administrative fine.
2. AI systems subject to notification, registration, or licensing	The development and deployment of prescribed AI systems may be subject to notification, registration, or licensing requirements under a future law, where such AI systems: - Affect public safety, financial or commercial security - Prevent harm to the public *No examples of AI systems have been provided yet.	Notify, register, or obtain a license with the regulator before developing or deploying the prescribed AI systems.	Civil liability No prescribed administrative fine.
3. High-risk AI systems	Prescribed High-risk AI systems, where the deployment of such systems affect: - State security - Health - Environment - Energy - Communication and telecommunications	The provider and deployer of high-risk AI systems will be subject to various statutory obligations, including risk management, documentation, human oversight, record-keeping, damage mitigation, incident notification, local coordinator/representative appointment, and regulatory cooperation.	Civil liability Administrative fine of up to THB 1 million (approx. USD 30,000). Administrative process - Corrective action orders - Court-ordered suspension of service

Type	Regulated AI	Key obligations	Legal sanctions
	- Transport and logistics - Public utilities		or deployment, or product recall - Court-ordered ISP blocking for non-compliant provider or deployer
4. AI systems with transparency obligations	AI systems capable of creating or modifying content that could mislead the public into believing it is real (e.g., deepfake/chatbot).	Comply with statutory obligations. The obligations vary depending on the positions in the supply chain: • Developer • Any person publishing the created or modified content • Deployer • Platform service provider Key obligations include risk assessment and mitigation, AI-content labelling and disclosure, user notification mechanism, record-keeping, and continuous improvement of AI-content risk management.	Civil liability Administrative fine of up to THB 3 million (approx. USD 90,000). Administrative process - Corrective action orders - Court-ordered suspension of service or deployment, or product recall - Court-ordered ISP blocking for non-compliant provider or deployer

Government AI

Government agencies that use AI systems to provide public services would be subject to specific obligations, *e.g.*, disclosing information about the AI system, its intended use, affected individuals, and any ethical impacts. The Digital Government Development Agency (DGA) will maintain a public register of AI systems used in government services, including any systems that have been removed from the register and the reasons for their removal.

Penalty and enforcement

The Draft AI Act adopts a progressive enforcement approach. In many cases, regulators would first have the ability to require businesses to remedy non-compliance before seeking more serious enforcement measures. However, the consequences of continued non-compliance can be significant, particularly for providers and deployers of regulated AI systems.

The Draft AI Act's enforcement toolkit goes well beyond administrative fines. Depending on the circumstances, regulators may seek service suspension, suspension of AI deployment, product recalls, or ultimately court-ordered blocking of AI systems in Thailand. In cases involving serious incidents affecting public safety, economic security, or national security, regulators may also exercise expedited intervention powers.

As a result, compliance under the Draft AI Act should not be viewed solely as a financial risk. The potential operational impact of service disruption, deployment restrictions, and regulatory intervention may be equally significant for businesses developing, supplying, or deploying AI systems in Thailand.

2. Training data and personal data

The Draft AI Act does not provide for an exception from copyright infringement for reproductions and extractions of data for scientific research purposes, including AI model training, similar to the text and data mining provision in the European Union's Directive (EU) 2019/790. Nonetheless, the Draft AI Act touches on the following when it comes to data used for training AI models:

- **Government's access to training data:** Regulator may seek a court order for accessing all the technical documents relating to AI system development, including training data, validation data, and testing data, for the purpose of preventing, responding to, and minimizing the risks from a serious incident.
- **Compulsory data sharing by state agencies to AI sandbox participants:** Business operators participating in an AI sandbox program could benefit from access to data shared by Thai state agencies, as well as exemptions from the enforcement for certain legal liabilities. However, participants remain liable for third-party damage.

For sandbox testing conducted for certain specified public-interest purposes, the Commission may order state agencies to hand over personal data to private-sector sandbox testing participants. Such transfer of personal data is permitted only when AI system development cannot be effectively fulfilled by processing anonymized, synthetic, or other non-personal data. Additional safeguards include participant obligations to implement effective supervision measures to identify the risks affecting the data subject's right and freedom in the course of AI system development, including ensuring such data processing activities do not lead to decisions affecting data subjects.

3. Business end users of GenAI are subject to disclosure requirements

The Draft AI Act introduces specific transparency requirements for AI-generated content, including deepfakes and AI chatbots. AI developers would be required to implement measures that allow AI-generated content to be identified, while platform operators would need to label such content, assess related risks, and provide reporting mechanisms for harmful or misleading content.

The highlight part is that **any person** — including an individual employee or user — who posts AI-generated or AI-altered content on sensitive topics (e.g., state security, election, regulated investments, food and drug properties, impersonation, or any illegal acts to be prescribed) must disclose that they use AI. Artistic, satirical, fictional, or similar content in media such as films, audiovisual works, or programs is subject to less stringent disclosure obligations.

This means that users must assess whether their AI-generated or AI-modified content falls within the prescribed categories and make the required disclosures before publication. AI providers and platform operators that provide effective disclosure tools and compliance mechanisms may gain a competitive advantage by enabling users to meet these obligations more easily.

4. Local representative with unlimited liability

For certain high-risk AI systems, overseas providers serving users or deployers in Thailand may be required to appoint a Thailand-based coordinator. In addition, future regulations may require providers of certain AI systems to appoint a local representative authorized to act on the provider's behalf, potentially without limitation of liability.

Businesses would therefore need to consider which local affiliate or partner is prepared to assume this role and how the associated risks should be allocated.

5. Data localization and controlled contracts

The Draft AI Act gives regulators additional oversight over AI services provided to government agencies and critical information infrastructure (CII) operators. Certain AI development, AI service, and AI data-processing activities may be designated as "controlled-contract" businesses.

If designated, regulators may prescribe mandatory contractual terms covering areas such as data processing, cross-border data transfers, risk management, security measures, changes to contractual terms, and termination rights. Importantly, these prescribed terms may be deemed to form part of a contract even if they are not expressly included by the parties.

The Draft AI Act also allows regulators to require certain AI services used by government agencies and CII operators to process data within Thailand.

As a result, AI vendors serving Thai government agencies, state-enterprises, or CII pipelines should proactively review their current MSAs and cloud terms to ensure readiness for the new regulatory requirements and evaluate Thailand-hosted or on-premises data processing solutions to address potential data localization requirements.

6. Serious incidents: Investigation, notification, suspension, and recall obligations

The Draft AI Act grants regulators broad powers to respond to serious AI-related incidents that may affect national security, economic security, or public safety. In certain circumstances, regulators may order the suspension of services or the recall

of AI systems without prior court approval. Providers and deployers may also be required to cooperate in investigating the incident and reporting their findings.

The Draft AI Act further allows regulators, with court approval, to obtain extensive information relating to the AI system, including technical documentation and training, validation, and testing data.

The Draft AI Act does not currently specify safeguards for trade secrets. Confidentiality provisions for models and datasets should therefore be considered in light of these potential regulatory access powers. The joint investigation obligation between providers and deployers may also require careful assessment.

7. Strict liability may extend across the value chain

The Draft AI Act introduces a broad and strict liability framework. Any person who fails to comply with the Draft AI Act and causes harm to another party must compensate the injured party jointly with other breaching parties, regardless of whether the breach is intentional or negligent. Available defenses are limited. Damages may also include costs incurred in preventing or mitigating harm.

As a result, liability may no longer be confined to a single participant in the AI ecosystem. AI developers, providers, deployers, platform operators, and other stakeholders may need to revisit their governance frameworks, contractual arrangements, indemnities, liability caps, audit rights, and insurance coverage to ensure risks are appropriately allocated across the AI value chain.

Next steps

1. **Take part in the hearing.** The Draft AI Act is now open for public consultation through law.go.th, until 14 August 2026. Businesses should review the proposed framework and consider submitting comments. Consultation materials and submission details are available on law.go.th.
2. **Map your roles.** The Draft AI Act imposes different obligations on providers, deployers, developers, and platform operators, and applies to certain offshore operations for high-risk AI. Even users are subject to disclosure obligations. It is prudent to start mapping your role in the AI supply chain, given the potential regulation approach introduced by the Draft AI Act.
3. **Review your governance, contracting, dawn raid, data sharing, and risk-allocation frameworks.** The Draft AI Act introduces broad compliance obligations, a joint liability regime, transparency requirements, and potential court-ordered regulatory access powers that may affect your AI governance models, incident-response procedures, data sharing agreements, and AI-related contractual arrangements.
4. **Prepare for AI-content labelling.** Businesses using or hosting AI-generated content should consider the practical implications of AI-generated content disclosure (e.g., AI labelling and marking) and illegal AI-generated content reporting channels and mechanisms.
5. **Pay particular attention to enforcement powers.** In addition to administrative fines, the Draft AI Act contemplates service suspension, product recalls, suspension of AI deployment, and ultimately, court-ordered blocking of AI systems in Thailand, which may have significant operational implications.
6. **Be a first mover: turn compliance into a competitive advantage.** Organizations that invest early in AI compliance, governance, and transparency may not only reduce regulatory risk but also differentiate themselves in the market by demonstrating responsible AI practices and becoming preferred partners for customers and stakeholders seeking trustworthy AI solutions in Thailand.

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



Chanaporn Anurukwongkul

Associate

chanaporn.anurukwongkul
@bakermckenzie.com



Pimpisa Ardborirak

Associate

pimpisa.ardborirak
@bakermckenzie.com



Chayapisa Kositbenjapol

Associate

chayapisa.kositbenjapol
@bakermckenzie.com



Phocharaphol Yingamphol

Associate

phocharaphol.yingamphol
@bakermckenzie.com



Nattachai Sumreongwong

Associate

nattachai.sumreongwong
@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.

