

15 October 2026

BSA RECOMMENDATIONS FOR THE DRAFT DIGITAL INFRASTRUCTURE SERVICES ACT

On behalf of the Business Software Alliance (**BSA**),¹ we appreciate the opportunity to provide our recommendations to the House of Representatives and to the Ministry of Digital Economy and Society (**MDES**) on the Draft Digital Infrastructure Service Business Act (**Draft Act**), proposed by Mr. Supachai Jaisamut and other Members of the House of Representatives. BSA has engaged extensively on digital policy in Thailand, including submitting comments on the draft notifications on cross-border transfers of personal data under the Personal Data Protection Act (**PDPA**) in 2023,² the Draft AI Bill in 2023,³ the Draft Platform Economy Act in 2024,⁴ the Draft Principles of the AI Law in 2025,⁵ the draft amendments to the Cybersecurity Act in 2025,⁶ and, most recently, the Draft Artificial Intelligence Act in August 2026.⁷

BSA is the global trade association of the enterprise software industry. Our member companies are leaders in artificial intelligence, cybersecurity, cloud computing, and other cutting-edge technologies. BSA members have made significant, long-term investments in cloud and data center infrastructure in Thailand and share the Government's ambition to strengthen Thailand's digital and AI capabilities. BSA offers our extensive global experience in technology policy to serve as a resource, and we hope that our recommendations below will be helpful as you develop a legal framework that supports secure, resilient, and sustainable digital infrastructure in Thailand.

BSA supports the Draft Act's objectives of protecting data and strengthening trust in digital services. Our recommendations focus on how these objectives can be achieved through measures that are proportionate, avoid duplication with existing Thai laws, and preserve Thailand's attractiveness as a destination for digital infrastructure investment.

¹ BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Morisawa, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

² BSA Comments on Draft Notifications on the Protection of Personal Data Transferred to a Foreign Country Pursuant to the Personal Data Protection Act 2019, 10 November 2023, at <https://www.bsa.org/policy-filings/thailand-comments-on-draft-notifications-on-the-protection-of-personal-data-transferred-to-a-foreign-country-pursuant-to-the-personal-data-protection-act-2019>.

³ BSA Comments on Draft Artificial Intelligence Bill, 18 August 2023, at <https://www.bsa.org/policy-filings/thailand-bsa-comments-on-draft-bill-on-promotion-and-support-of-national-artificial-intelligence-innovation>

⁴ BSA Comments on the Draft Platform Economy Act, 30 April 2024, at <https://www.bsa.org/policy-filings/thailand-bsa-comments-on-thai-draft-platform-economy-act>.

⁵ BSA Recommendations for Draft Principles of the Law on Artificial Intelligence, 7 June 2025, at <https://www.bsa.org/policy-filings/thailand-bsa-recommendations-for-draft-principles-of-the-law-on-artificial-intelligence>.

⁶ BSA Comments on Draft Amendments to National Cybersecurity Law, 15 August 2025, at <https://www.bsa.org/policy-filings/thailand-bsa-comments-on-draft-amendments-to-national-cybersecurity-law>.

⁷ BSA Recommendations for the Draft Artificial Intelligence Act, 14 August 2026, at <https://www.bsa.org/policy-filings/thailand-bsa-recommendations-for-the-draft-artificial-intelligence-act>.

Definitions and Scope

Definitions. Section 3 defines “cloud services” as services for receiving, transmitting, processing, and storing electronic data through a telecommunications network for non-affiliated persons, using a data center located in Thailand. The definition does not distinguish between Infrastructure-as-a-Service (**IaaS**), Platform-as-a-Service (**PaaS**), and Software-as-a-Service (**SaaS**). These services differ significantly in their offerings related to physical infrastructure and in the degree of control the service provider exercises over customer data. Section 3 also allows “other services” to be brought into scope by Ministerial Regulation but does not include criteria for which services may be added. This creates significant uncertainty for businesses serving, or planning to serve, the Thai market.

The scope of the Draft Act penalizes investment in Thailand. As the definition of cloud services applies only to services using a data center located in Thailand, a provider that invests in Thai data centers to serve the Thai customers would be subject to licensing, data localization, and criminal liability. This creates a direct disincentive to build or expand cloud and data center infrastructure in Thailand, which runs counter to the Government's investment promotion objectives.

Licensing without thresholds. Section 5 requires every business operator to obtain a license from the Minister, regardless of whether it provides IaaS, PaaS, or SaaS. Under this definition, every provider of cloud services using a data center in Thailand would require a license, from large infrastructure providers to small software companies. This would add unnecessary compliance costs for businesses, especially small and medium enterprises. It would also create a significant administrative burden for the authorities that must process and supervise those licenses.

An untargeted licensing requirement will not advance the Draft Act's stated objectives. The concerns about energy security, water resources, and environmental impacts arise from the physical operation of large data centers. Chapter 2 of the Draft Act already addresses these concerns, as do existing energy, environmental, and town planning laws. Licensing the software and platform services that run in those facilities would not reduce their electricity or water consumption. The protection of data is likewise already governed by the PDPA and the Cybersecurity Act.

Also, many services in scope are already subject to sector-specific oversight in Thailand. An additional Ministerial license would layer a further authorization on top of these regimes, creating overlapping obligations, inconsistent requirements, and uncertainty as to which authority has primary responsibility.

Resellers and partners. Cloud services are frequently delivered to Thai customers through resellers, system integrators, and managed service providers. As drafted, each of these parties could be treated as a separate “business operator” requiring its own license, even where the underlying service is provided by a licensed operator. This would multiply licensing obligations across the supply chain without any corresponding benefit.

Recommendations:

- Remove the licensing requirement in Section 5. If a licensing requirement is retained, apply it only to specific business operators of concern, with clearly defined thresholds, for example, data centers above a clearly defined capacity threshold, or specific, objectively defined services that serve critical functions directly related to national security. Avoid duplicated licensing across IaaS, PaaS and SaaS layers. Resellers, system integrators, and managed service providers delivering a service of a licensed or notified operator should not require a separate license.

- Narrow the definition of “digital platform services” so that they are only subject to regulatory obligations such as licensing only where a clearly identified regulatory gap and demonstrable risk justify additional oversight. Services and operators already regulated under the MDES or sector regulators should not be subject to duplicative licensing or other obligations.
- Require published criteria and public consultation with industry before any new service category is added by Ministerial Regulation under Section 3.

Data Localization and Data Sovereignty

Section 6 requires business operators to store personal data of Thai nationals, data of Thai-incorporated legal persons, and government information in Thailand. Transfer, processing, or backup abroad is permitted only for “reasons of necessity,” under rules to be prescribed by Ministerial Regulation.

The scope of Section 6 is broad. It extends to non-personal data of any Thai-incorporated company, which would cover almost all data that enterprise service providers handle for their Thai business customers. It applies a nationality test that is not applied in the PDPA and that service providers have no practical way to apply. It also restricts offshore processing, backup, and storage.

It is inadvisable to localize broad categories of data encompassing routine commercial, personal and non-personal data or proprietary information used in everyday business operations. Such data does not generally present the same national security risks as highly sensitive government information, such as classified military or intelligence data. Applying the same restrictions regardless of sensitivity or risk would impose disproportionate costs, hinder ordinary business operations and access to global services, and divert company resources from protecting data that genuinely warrants heightened safeguards. Thailand should therefore avoid unnecessary restrictions on routine commercial data and adopt a targeted, risk-based approach limited to clearly defined categories of data with a direct nexus to national security.

Section 6 introduces a separate layer that is inconsistent with the cross-border transfer framework under Sections 28 and 29 of the PDPA and creates an additional authority regulating such transfers. Section 6 places liability on business operators such as cloud providers, which typically act as data processors, for transfers their customers may lawfully make as data controllers. Obligations should fall appropriately on the party that is authorized to decide how data is processed and able to take responsibility for that decision, i.e., generally the data controller under the PDPA. It is also unclear how this broad data localization mandate will interact with the classification of data and information systems under the National Cyber Security Agency’s (**NCSA**) Cloud Security Standard and the Digital Government Agency’s (**DGA**) proposed Government Data Classification, which do not require localization of all government data.

Cross-border data transfers underpin the global economy and are vital to the security of networks and information systems. Data localization requirements do not ensure information security and are likely to have the opposite effect of reducing information security. Amongst others, robust and effective payment security, fraud prevention, anti-money laundering controls, and cyber threat detection depend on analyzing information across multiple jurisdictions. For example, effective fraud detection systems rely on large, diverse, and real-time global transaction datasets to identify patterns, improve risk scoring, and coordinate timely responses to emerging fraud typologies. AI development similarly depends on diverse datasets and advanced computing resources often hosted internationally. Restrictions on these data transfers will reduce

effectiveness and resilience, undermining consumer protection, financial system integrity, cross-sector innovation, and trust in the digital economy.

True resilience depends on globally distributed and redundant infrastructures and trusted international data transfers. Mandatory in-country storage and backup would prevent this and would prevent security tools from drawing on threat intelligence first observed elsewhere. Thailand's own Digital Government Strategy and Cloud First Policy actively encourage government agencies to adopt cloud-based enterprise software. The Draft Act's licensing requirements and data localization rules would create legal uncertainty for cloud deployments, thereby slowing or reversing the Government's own modernization agenda.

Localization is also neither necessary nor sufficient to secure data sovereignty. What matters for sovereignty is the ability to govern, audit, and mitigate risk, not the geographic location of data.⁸ Thailand already has these tools, including the PDPA and its enforcement mechanisms, transparent contracts, legal safeguards, and technical measures such as encryption and pseudonymization.

Data localization requirements also have a chilling effect on investment, including the data center and cloud investment that Thailand is actively attracting. Section 6 would also be difficult to reconcile with the cross-border data flow provisions of the ASEAN Digital Economy Framework Agreement (**DEFA**), which is due to be signed in November 2026.

Recommendations:

- Delete Section 6 and rely on the PDPA framework for cross-border transfers.
- If Section 6 is retained, limit data localization to sensitive government data with a direct nexus to national security, specified in a published list supported by a risk assessment. Data localization obligations should only apply to the data controller, as defined in the PDPA, as the party that controls the data, rather than to the data processor, which acts strictly on instructions by the data controller.
- Allow transfers permitted under the PDPA and internationally recognized mechanisms, including binding corporate rules, standard contractual clauses, the Global Cross-Border Privacy Rules (**CBPR**), and other appropriate safeguards, without additional approval, notification, or other requirements.
- Permit offshore processing such as offshore remote administration and technical support, cross-border transfer of logs and threat intelligence for incident response, and encrypted backup and disaster recovery.

Exclude Enterprise Services from Suspension of Access Requirements

Section 19 requires licensed cloud service providers to verify the identity of their cloud service users “for the purpose of maintaining public order and good morals.” Where there are reasonable grounds to believe that a user is breaching any law, a competent official may order the provider to suspend access to specified data. The order is sent by email and must be complied with within 12 hours, without a court order. Given this rationale, it appears that Section 19 is expected to apply primarily to consumer-facing services that directly interact with individual end-users.

Enterprise services are intended for organizations of all sizes and across all industries. Enterprise service providers typically do not interact with the individual end users served by their enterprise customers, and do not have direct control over their actions. Their access to and knowledge of customer data is frequently limited by privacy and security controls built into enterprise products.

⁸ Digital Sovereignty for Governments and Enterprises, 30 September 2026 at <https://www.bsa.org/policy-filings/global-digital-sovereignty-for-governments-and-enterprises>.

Furthermore, where customers deploy customer-controlled encryption keys, cloud providers do not hold their decryption keys. An enterprise service provider is therefore generally unable to suspend access to specific data within a customer's environment. Requests to access or block data must be directed to the data controller. In practice, an order to the data processor would suspend the customer's entire service, disrupting hospitals, banks, government agencies, and other organizations. Complying with such orders could also place providers in breach of their contractual and other legal obligations. Similarly, enterprise customers are organizations under contract with the provider, therefore user identity verification serves little purpose.

Regulations in other jurisdictions distinguish between consumer and enterprise services. For example, Singapore's Online Safety Act⁹ includes a code of practice for Social Media Services, where there is a direct relationship between the platform and consumers. Australia's Online Safety Act¹⁰ follows a similar approach, and through codes of practice distinguishes between enterprise and consumer services.

Recommendations:

- Delete Section 19 from the Draft Bill as it is unworkable for data processors to verify the identity of Thai consumer and restrict access to their own data on the order of an official without clear legal bases.
- If retained, exclude enterprise services from Section 19 and from the scope of "cloud services" and "digital platform services" in Section 3 and include a provision to exclude services primarily designed for and used by enterprise customers. For services remaining in scope, require a court order before access to data is suspended. Orders should be directed first to the data controller, and should provide a reasonable period for compliance, notice to affected customers, and a right of appeal.

Liability and Penalties

The Draft Act imposes criminal liability, including imprisonment of up to five years, for operating without a license, in addition to periodic penalty payments per day of non-compliance (Section 27). Failure to store data in Thailand carries imprisonment of up to three years (Section 28). In addition, both provisions set minimum fines with no maximum cap. These penalties are disproportionate to what are in substance administrative and compliance failures. They are also more severe than those for most breaches of the PDPA, which relies primarily on administrative fines. Severe criminal penalties of this kind would deter investment in Thailand's digital infrastructure. The Draft Act already provides for regulatory fines for other obligations (Sections 30 to 35), and that approach should apply consistently.

Recommendations:

- Replace criminal sanctions with administrative fines with stated maximum amounts, aligned with the PDPA.
- Require the authorities to notify the business operator of the non-compliance and provide a reasonable period to correct it before imposing penalties.

Other Concerns

Local Staffing and Local Content. Section 7 requires that at least half of all personnel performing system supervision duties be Thai nationals. Section 8 allows the Minister to prescribe proportions of domestically manufactured materials or equipment. These requirements would

⁹ Singapore Online Safety (Miscellaneous Amendments) Act 2022, 21 Dec 2022, <https://sso.agc.gov.sg/Acts-Supp/38-2022/Published/20221221?DocDate=20221221>.

¹⁰ Australia Online Safety Act 2021, Jan 23, 2022, <https://www.legislation.gov.au/C2021A00076/latest/text>.

restrict access to global expertise and technology without advancing the Draft Act's objectives. This would directly affect the network, compute, and storage equipment used in data centers, much of which may be sourced from global supply chains rather than domestically manufactured in Thailand. Equipment connected to networks in Thailand is also already subject to NBTC technical standards, so a separate domestic content requirement would add cost and supply constraints without improving security or quality.

Recommendation: Delete Sections 7 and 8.

Powers of Competent Officials. Section 26 allows competent officials to enter the premises of a business operator, inspect, access and seize computer systems, and order directors, employees, auditors, and other persons to give statements and produce evidence.

None of these powers requires a court order or other valid legal process, which are essential safeguards for the rights of individuals and companies when government officials exercise their lawful functions. For cloud services, the same systems host data for many customers, therefore the exercise of these powers could affect customers that are not connected with the matter under investigation. Additionally, this requirement could raise concerns under internationally accepted standards on government access to data (e.g., OECD's Declaration on Government Access to Personal Data Held by Private Sector Entities; Thailand is not an OECD member yet but is an official accession candidate).

Recommendation: Delete Section 26. If it is retained, require a court order before competent officials may enter premises, inspect or seize documents or data, or compel individuals to give statements. Competent officials should also be required to protect customer data held by service providers. Prohibit the seizure of hardware connected to multi-tenant infrastructure to preserve the data of other users unconnected to the investigation.

Transition Period. Existing operators must apply for a license within 180 days of the relevant Ministerial Regulation taking effect. The obligations under the Draft Act depend on subordinate instruments that will follow it. As drafted, this period may expire before organizations know what compliance requires.

Recommendation: Provide a minimum transition period of 12 to 18 months after the publication of the relevant implementing measures.

Conclusion

BSA thanks the House of Representatives and the MDES for considering our recommendations on the Draft Act. We share the objectives of ensuring that Thailand's digital infrastructure is secure, resilient, and sustainable, and that data is well protected. We hope our comments will help achieve these objectives in a manner that is consistent with Thailand's existing legal frameworks, including the PDPA, and that supports continued investment in Thailand's digital economy. BSA welcomes the opportunity to serve as a resource on international developments and best practices in digital infrastructure and data governance. Please do not hesitate to contact me at waisanw@bsa.org if you have any questions regarding our recommendations. Thank you once more for your time and consideration.

Yours sincerely,

Wong Wai San
Director, Policy – APAC