



# GLOBAL DATA ALLIANCE

## TRUST ACROSS BORDERS

## SUBMISSION ON THAILAND DRAFT DIGITAL INFRASTRUCTURE SERVICES ACT TO THE HOUSE OF REPRESENTATIVES AND THE MINISTRY OF DIGITAL ECONOMY AND SOCIETY

15 October 2026

The Global Data Alliance (**GDA**)<sup>1</sup> appreciates the opportunity to provide our recommendations to the House of Representatives and 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. The GDA has engaged extensively on data governance issues in Thailand, including comments submitted to MDES, the Electronic Transactions Development Agency, the Office of the Personal Data Protection Committee, and the National Cybersecurity Committee, among others.<sup>2</sup>

### About the Global Data Alliance

The GDA is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data responsibility. The GDA supports policies that help instill trust in the digital economy without imposing undue cross-border data restrictions or localization requirements that undermine artificial intelligence (**AI**), data security, cybersecurity, innovation, economic development, and international trade. Our members operate in every major sector of the economy, including agriculture, automotive, aviation, biopharmaceutical R&D, consumer goods, energy, financial services, healthcare, manufacturing, supply chain and logistics, telecommunications, and enterprise software. Given the GDA's focus on cross-border data, our comments focus on the data localization requirements of the Draft Act, together with related provisions on scope, local staffing and content, and penalties that would affect GDA members across sectors.

GDA member companies are significant investors in Thailand, investing billions of dollars and supporting thousands of jobs. Thailand's rapid emergence as a regional digital hub rests directly on the openness of its data environment. Thailand's Board of Investment recorded THB 521.2 billion (approximately US\$16 billion) in data center investment across 28 projects in the first half of 2025 alone. These figures – accounting only for data center investment – do not account for the even larger investments in AI-driven manufacturing and services across the many different sectors in which GDA member companies operate. Investment of this scale is committed against an expectation of a stable, technology-neutral, and internationally interoperable regulatory environment. Cross-border data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes, in every country, to create new kinds of jobs, boost efficiency, drive quality, and improve output.

### 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

<sup>1</sup> For more information on the Global Data Alliance, please see [www.globaldataalliance.org](http://www.globaldataalliance.org)

<sup>2</sup> For more information on the GDA's prior engagements with the Kingdom of Thailand, please see submissions filed here: [https://globaldataalliance.org/resources-results/?pub\\_type=resource-filings&location=loc-thailand&sector=&language=&posts\\_filtered=1](https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-thailand&sector=&language=&posts_filtered=1)

“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 Personal Data Protection Act (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.<sup>3</sup> 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

<sup>3</sup> Digital Sovereignty for Governments and Enterprises, 30 September 2026 at <https://www.bsa.org/policy-filings/global-digital-sovereignty-for-governments-and-enterprises>.

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.

## 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 restrict access to global expertise and technology without advancing the Draft Act's objectives.

**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.

*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

The GDA shares the Draft Act's objectives of protecting data and strengthening trust in digital services, and our comments above are offered in that spirit. However, the Draft Act is unnecessary to ensure that regulation remains risk-based, technology-neutral and proportionate as these are already carefully considered and reflected in existing laws governing data and infrastructure operators. Thailand's framework should avoid duplicative licensing, preserve cross-border data transfers, provide legal certainty for investors, and align with internationally recognized standards. We thank the House of Representatives and MDES for considering these comments. We encourage continued dialogue with the private sector, with sufficient time for consultation, so as to achieve common goals for secure, resilient, and internationally interoperable digital infrastructure in Thailand. Please do not hesitate to contact us if you require any clarification or further information.

Yours sincerely,

**Joseph P. Whitlock**  
Executive Director  
Global Data Alliance  
josephw@bsa.org