GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

MAY 13, 2024

GDA COMMENTS TO THAILAND'S NATIONAL CYBERSECURITY COMMITTEE

STANDARDS FOR MAINTAINING CYBERSECURITY IN CLOUD SYSTEMS

The Global Data Alliance (GDA)[1] welcomes the opportunity to offer comments on the Announcement of Thailand's National CyberSecurity Committee on Standards for Maintaining CyberSecurity in Cloud Systems (*hereainafter* "Cloud Security Policy").[2]

The GDA is a cross-industry coalition of companies, headquartered across Asia, Europe, and the Western Hemisphere, that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. The GDA supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade.

GDA member companies are active in many sectors of Thailand's economy. GDA members collectively support hundreds of thousands of jobs, hundreds of millions of dollars in investment, and activities to advance innovation and economic development in Thailand.

The GDA supports many aspects of Thailand's Cloud Security Policy, but recommends that Thailand explore alternative approaches to the cloud infrastructure and data localization mandates found therein.[3]

Overall Comments and Recommendations

The GDA strongly supports Thailand's goal of improving cloud security and integrity via the Cloud Security Policy. The GDA also supports Thailand's incorporation of international standards throughout the Cloud Security Policy. The GDA respectfully submits that the Cloud Security Policy will be most effective if it reflects a shared responsibility between Thai government cloud service customers and cloud service providers to use best practices to manage risk and improve cloud resiliency.

At the same time, the GDA is concerned that the Cloud Security Policy appears to contain local data storage mandates that will impede the Policy's stated goals of improving security. The GDA is also concerned with provisions that indicate that backup servers should be located in: (1) Thailand, (2) elsewhere in Southeast Asia, or (3) Hong Kong, China.

The Cloud Computing Scorecard (a global report that ranks countries' preparedness for the adoption and growth of cloud computing services) explains that:

> Cloud services operate across national boundaries, and their success depends on access to regional and global markets. Restrictive policies that create actual or potential trade barriers will inhibit or slow the evolution of cloud computing.[4]

We respectfully suggest that the Cloud Security Policy be revised to embrace the full potential of cloud computing through an approach that is flexible, promotes privacy and security, and allows enterprises in Thailand to benefit

from cross-border access to best-in-class cloud-delivered infrastructure, software, and technology. In particular, we recommend that Thailand explore alternative approaches to the data storage mandates found in the draft Policy.

Discussion

The Cloud Security Policy contains the following provision that requires the establishment of a "main data center" in Thailand, and a "backup data center" in Thailand, the Hong Kong Special Administrative Region, or elsewhere in Southeast Asia. Specifically, Article 5.2.5 states as follows:

> 5.2.5 Physical and environment security
> 5.2.5.1 Location of data centers (Data Center Location)
>
> Cloud Service Users
>
> a) Should use the main data center in Thailand (data localization)
>
> Cloud Service Provider
>
> a) A main data center should be established in Thailand (data localization).
>
> b) A backup data center should be established in Thailand (data localization) or in Southeast Asia that is as close to the main use of cloud service users as possible, including the Hong Kong Special Administrative Region

The GDA has several concerns with the operational and security risks associated with this infrastructure and data localization mandate, particularly relative to Thailand's cybersecurity objectives and its interest in secure cloud computing infrastructure and the enabling technologies they support.

The cross-border data restrictions in the draft Policy may also undermine public policy goals relating to the health, privacy, and security of persons in Thailand. We address these topics below.[5]

- **Impact on ICT Policies:** ICT policies can help coordinate public-private dialogue, support investment, and maximize the benefits of ICT technologies across the economy. Cross-border data restrictions often undermine these polices. For example, the benefits of cloud computing policies policy are most likely to arise in a cross-border context that allows for elastic and scalable delivery of computing resources, rapid load balancing, and ready access to best-in-class technology from all over the world. Using data localization mandates and transfer restrictions to ban cross-border access to cloud computing infrastructure and technology would deprive local enterprises (including MSMEs) and users of:
    - Cross-border access to IT resources hosted abroad;
    - Cross-border collaboration and communication with foreign business partners;
    - Foreign transactions and business opportunities; and
    - Improved resiliency resulting from data storage across multiple geographical locations.[6]

- **Impact on Cybersecurity**: Some argue that cross-border data restrictions are necessary to ensure cybersecurity. However, *how* data is protected is more important to security than *where* it is stored, and transfer restrictions often result in *weaker*, not *stronger*, cybersecurity. Cross-border data transfers help improve cybersecurity because these transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Stronger cybersecurity is enabled by cross-border data analytics, an assertive cyber-defense posture coordinated across IT networks and national boundaries.[7] When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities.[8] Please see Annex I for more information.

- **Impact on Privacy**: Some argue that cross-border data restrictions are necessary for privacy reasons – i.e., to ensure that companies process and use data consistent with a country's data protection laws. In fact, organizations that transfer data globally typically implement procedures to ensure that the data is protected even when transferred outside of the country. To that end, organizations often rely on various approved data transfer mechanisms.[9]
- **Impact on Regulatory Compliance**: Some claim that cross-border data restrictions ensure governmental access to data for regulatory or investigatory purposes. The location of the data, however, is not the determining factor. On the contrary, "data localization requirements can increase … operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information." [10] Accordingly, regulatory authorities in many countries actually encourage the responsible transfer of data across borders.[11] Likewise, data transfers are critical to other public policy priorities, including financial fraud monitoring and prevention; anti-money laundering; anti-corruption; and other legal compliance objectives.

In addition, we note that the table at page 6 provides a framework that classifies cloud services as Low, Intermediate and High level of impact. However, there is no clear guidance on how each agency would determine what the proper classification is. It would be helpful to provide greater transparency on how such classification would be made to ensure consistency of classification and to avoid potential issues with under or over classification. We also recommend that there be an avenue to request for decisions on classifications to be reviewed or reconsidered based on inputs received.

Given the classification, it may also be worthwhile for consideration to be given to differentiate the localization requirements based on the classification level. For instance, systems under the low impact classification may be exempt from any localization requirements. Consideration should also be given to distinguish different treatment based on the type of cloud service provider (e.g., Infrastructure-as-a-Service, Platform-as-a-Service). It may not be necessary to subject Software-as-a-Service, which could broadly include any Internet-offered service within the scope of the localization requirements.

Detailed Recommendations

We offer the following detailed recommendations:

- **Our primary recommendation** is for Thailand's National Cybersecurity Committee to delete Article 5.2.5.1 (Data Center Location) from the Cloud Security Policy.
- **Our alternative recommendations** would be for Thailand's National Cybersecurity Committee to clarify that data centers under this Article may be located in any economy in which the cloud service provider is able to meet the Committee's functional and technical cybersecurity requirements based on a demonstrated risk management plan.

In either case, we urge the National Cybersecurity Committee to remove the reference to Hong Kong Special Administrative Region because of widespread concerns regarding the security and integrity of data – both from a cybersecurity and a legal due process perspective – that is subject to the jurisdiction of the People's Republic of China.

Conclusion

In conclusion, we respectfully recommend that Thailand remove the draft Policy's local infrastructure and data localization mandates from the Cloud Security Policy. We appreciate the opportunity to share these views and hope that they will be helpful as Thailand considers its next steps on the draft Policy. Please do not hesitate to contact us with any questions regarding this submission.

Annex

The Relationship Between Cybersecurity & Local Infrastructure Mandates, Data Localization Mandates, and Cross-Border Data Transfer Restrictions

The ability to locate and transfer data in the most functionally secure manner is a cybersecurity risk management best practice. This is in part because cross-border visibility into cyber-related data allows for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Additionally, companies may choose to store data at geographically diverse locations to obscure the location of data and reduce risk of physical attacks, to enable companies to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location. Conversely, when governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities, as summarized below:

- **Integrated Cybersecurity Planning.** Data transfer restrictions and localization requirements force organizations to adopt a siloed approach to data, often restricting the locus of certain data, but not others. This differentiation creates unnecessary technical complexity without any corresponding benefit to security. Simply put: artificial requirements to store data within borders strain the people, processes, and technologies an organization needs to manage its cybersecurity risk.

- **Cybersecurity Awareness.** Data transfer restrictions and localization requirements impede visibility of cybersecurity risks, not only at the intra- and inter-organizational levels, but also at national and international levels. If cyber defenders cannot access threat indicators or other cybersecurity data collected in one jurisdiction, it becomes harder to address malicious cyber activity in other jurisdictions.

- **Cybersecurity Collaboration.** Data transfer restrictions and localization requirements can impede cross-border collaboration, information sharing, and other coordinated network defense. When such restrictions and requirements isolate network defenders from each other, they cannot adopt a unified and coordinated defensive posture against malicious actors that do not respect national borders. In short, data transfer restrictions can give malicious actors that do not respect local legal requirements a lasting structural advantage over cyber defenders that do.

- **Third-Party Cybersecurity Services.** Many organizations amplify their own cybersecurity risk management through third-party cybersecurity service providers. Best-in-class services depend on access to cyber data from around the globe. Without this access, these services and their users become more vulnerable to compromise.

- **Cybersecurity Resiliency.** Whether a particular geographic area is at high risk for a natural disaster or in a potential future war zone, having data efficiently distributed is a crucial component of resiliency. The misconception that keeping data only within national boundaries will increase its security can actually create significantly more risk.

- **Protectionism in the Name of Cybersecurity.** Localizing data within a country—or blocking its transfer—has no functional cybersecurity benefit. Security is determined by the technical and operational protections that accompany the data, not the location. Transfer restrictions and localization requirements are often used to advance other objectives. Perhaps the most systemic problem with using cybersecurity laws to require localization, then, is that it diminishes the role of laws and policies that are truly designed to improve security.

[1] GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. GDA member companies have operations and support millions of jobs across all 50 US states. For more information, see https://www.globaldataalliance.org

[2] https://www.law.go.th/listeningDetail?survey_id=MzcyNURHQV9MQVdfRlJPTlRFTkQ=

[3] GDA members hold a variety of views on other aspects of the draft Cloud Security Policy, which they may address through submissions via other organizations. Consistent with the GDA's cross-border data policy focus, the GDA's submission focuses on the data localization and data transfer aspects of the Policy alone.

[4] BSA, *Cloud Computing Scorecard*, p. 1 (2018), at https://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf

[5] For additional information, *see* https://www.globaldataalliance.org/downloads/02112020[]crossborderdata.pdf

[6] *See generally,* BSA, *Moving to the Cloud – A Primer on Cloud Computing* (2018), at https://www.bsa.org/files/reports/2018BSA_MovingtotheCloud.pdf.

[7] *See id.* Cloud services delivered across-borders provide security advantages over alternative IT delivery approaches (on-premises or local cloud services):

- Physical Security: Certified personnel can carefully monitor servers 24/7 to prevent physical breaches, and can apply consistent protocols over a small number of locations.
- Data Security: CSPs can ensure data integrity through use of state-of-the-art encryption protocols for data at-rest and in-transit. CSPs can establish redundant backups of data in geographically dispersed data centers, mitigating risk of loss in the event of power outages or natural or manmade disasters.
- Advanced Threat Detection: CSPs leverage state-of-the-art enhanced security intelligence They use regular penetration testing to simulate real-world attacks and evaluate security protocols against emerging threats.
- Automated Patch Deployment: Automated and centralized patch deployment and realtime updates to network security protocols work to protect systems from newly identified vulnerabilities.
- Incident Management and Response: CSPs maintain global teams of incident response professionals to respond and mitigate the effects of attacks and malicious activity.
- Certification: CSPs are typically certified to international security standards, and go through regular audits to maintain their certifications.

[8] *See id.,* p. 1.

[9] *See generally* footnote 8, *infra.* These data transfer mechanisms may include adequacy decisions, certifications, codes of conduct, Binding Corporate Rules (BCRs), and Standard Contractual Clauses (SCCs) that contain built-in data protection safeguards.

[10] *See e.g.,* United States-Singapore Joint Statement on Financial Services Data Connectivity, at: https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity;

[11] *See id.,* USMCA Art. 17.2.1; US-Japan FTA Art. (PPC).