October 28, 2025

Comments on the DICT Draft Circular on Data Residency of October 27, 2025

The Honorable Secretary Henry Rhoel Aguda
Department of Information and Communications Technology (DICT)
Carlos P. Garcia Avenue
Diliman, Quezon City 1101
Republic of the Philippines

Dear Secretary Aguda:

The Global Data Alliance ("GDA")[1] respectfully submits the following comments regarding the Department of Information and Communications Technology's ("DICT") *Policy Guidelines on Data Residency for Government Agencies* ("October 27 Policy Guidelines").

The GDA opposes the "data residency" features of the Guidelines, which apply broadly to both secret and sensitive government data. The GDA also opposes the "sovereign cloud" provisions that require "all secret, sensitive, and confidential government data will remain within Philippine territory or sovereign jurisdiction" and that restrict data transfers.

The GDA is also concerned with the process followed in publishing the draft Guidelines. On October 17, DICT had published a draft Circular that implied a much narrower scope of potential data restrictions. The GDA was generally supportive of the October 17 Circular.[2] Unfortunately, on October 27, DICT published – without warning – a wholly new set of guidelines, demanding that industry provide comments within a single day. The October 27 Guidelines mandate data residency (also known as "data localization") for a wide swath of government data sets and establish an unprecedented "sovereign cloud" certification framework. (The Guidelines also mandate that an even broader range of data be stored in data centers certified as Tier 3 or Tier 4 by the "Uptime Institute" or equivalent.)

The data localization mandates apply to data associated with:

> [D]epartments and agencies under the Executive Branch, State Universities and Colleges (SUCs), Government-Owned or -Controlled Corporations (GOCCs) and their subsidiaries, Government Financial Institutions (GFIs), Local Government Units (LGUs), and other government instrumentalities [and] cloud service providers, intermediaries, and other private entities with transactions, contracts, or data related to … cloud computing services for all covered government agencies.

We urge DICT to remove the data localization mandates, data transfer restrictions, and sovereign cloud provisions from the October 27 Guidelines. Alternatively, we urge DICT to revert to the approach outlined in the October 17 Circular. Additionally, we ask DICT to focus more broadly on open, voluntary, and international standards-based technical approaches for the handling of relevant data sets.

A. About the Global Data Alliance

The GDA is a cross-industry coalition of companies committed to high standards of data responsibility and to the trusted, secure, and interoperable movement of data across borders. The GDA supports policies that help instill trust in the digital economy without imposing undue cross-border data restrictions or localization requirements that undermine cybersecurity, innovation, economic development, and international trade.

GDA members support millions of dollars of investment and thousands of jobs in the Philippines. GDA members are also longstanding supporters of digital transformation and economic development in the Philippines powered by cross-border access to best-in-class technology, information, and know-how from around the world.

The GDA has engaged with the Philippine government to promote these objectives through GDA submissions made in October 2025, September 2025, March 2025, September 2024, April 2024, December 2023, September 2023, and September 2022. We have also met repeatedly with senior officials from the Government of the Philippines on these issues.

B. GDA Opposes the Restrictive Aspects of the October 27 Guidelines

The GDA opposes the broad data localization mandates and transfer restrictions found in the October 27 Guidelines, as well as those found in the "sovereign cloud" certification mandates. The GDA also questions the propriety of mandating the adoption of a single corporation's technical certification mandates, rather than adopting a more open and international standards-based approach.

The GDA had favored the more balanced approach reflected in the October 17 Circular. While the October 17 Circular had marked an improvement over earlier measures on which the GDA previously commented, the October 27 Guidelines regrettably revert to many of the unfavorable conditions outlined in many of the prior draft orders, including:

1. *Draft Policy Guidelines on Data Localization of Data Stored in the Cloud (2023)*
2. *Draft Department Circular on the Localization of Government Data (2024)*, and
3. *Workplan for Data Sovereignty and Data Localization for Data Governance (2025).*

The October 27 Guidelines – like those earlier measures – would impose strict data localization mandates and barriers to a wide range of cross-border data use, undermining the Philippines' strategic goals in digital transformation, cybersecurity, public health, and economic modernization.

1. Recommendations for Data Residency Provisions

We oppose the data residency requirements of the October 27 Guidelines. These restrictions will impose significant costs and risks on the Philippine government and citizenry. We urge DICT to remove these requirements from the October 27 Guidelines.

2. Recommendations for Data Transfer Provisions

We oppose the restrictions on cross-border data transfers in the October 27 Guidelines. Among other things, these restrictions will make it difficult, if not impossible, for the Philippines to apply AI or other computational data analytics to many Philippine government operations, given that relevant government data would need to be processed offshore for many available AI solutions. [3]

C. Conclusion

The October 27 Guidelines adopt an unworkable approach that will undermine Philippine cybersecurity, economic, technology, and security interests. We DICT to remove the highly restrictive elements of the Guidelines. Instead, we encourage the Philippines to explore an approach more closely aligned with prevailing international digital norms and best practices.

[1] For more information on the Global Data Alliance, please see: https://www.globaldataalliance.org/

[2] *Draft Department Circular on Data Residency,* dated October 17, 2025 (*hereinafter* "October 17 Circular").

[3] We encourage DICT to carefully review and benchmark its efforts against GDA's Cross-Border Data Policy Principles. These six principles, adopted by companies and policymakers around the world, articulate the key elements of a secure, trusted, and interoperable cross-border data environment:

1. There should be a strong presumption in favor of the seamless cross-border movement of data: Open and secure data flows enable innovation, growth, and cybersecurity while maintaining accountability through risk-based safeguards and technical protections.

2. Any limits on cross-border transfers must be proportionate, evidence-based, and no more restrictive than necessary to achieve a legitimate public policy purpose: Governments should adopt limitations on data transfers only when legally and demonstrably required to achieve legitimate public policy objectives, as supported by empirical analysis of risk.

3. Any limits should NOT serve as arbitrary, discriminatory or disguised restrictions on the movement of data: Legal frameworks should not discriminate among entities based on nationality or origin of the persons, technologies, service, or products involved.

4. Regulatory frameworks should align with international norms and best practices: Policies should be consistent with commitments made under multilateral and regional arrangements—including ASEAN, APEC, the OECD, and trade agreements such as the CPTPP, USMCA, or WTO JSI—to foster global trust and predictability.

5. Accountability models should be flexible and technology-neutral.
Organizations should be able to demonstrate compliance through varied mechanisms—such as certification, contracts, or audits—without being tied to specific technologies or geographic constraints.

6. Interoperability and trust should be the foundation of digital policy: Secure and predictable data flows rely on international cooperation, reciprocal trust, and regulatory interoperability that together promote innovation, national security, and resilience. Frameworks should also be designed to interoperate across jurisdictions to reduce regulatory friction and promote trade.