November 20, 2025

Comments on the Draft Executive Order of November 18, 2025

The Global Data Alliance ("GDA")[1] respectfully submits the following comments regarding the draft Executive Order Modernizing the Government Data Classification and Establishing Data Residency Policy Guidelines (draft dated Nov. 18, 2025) ("draft Executive Order").

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. Our members operate in every major economic sector, including manufacturing, financial services, logistics, health, energy, and technology. We believe that cross-border data flows are fundamental to economic growth, cybersecurity, scientific innovation, and the protection of public welfare.

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. Discussion – GDA Supports Many Aspects of the draft Executive Order

The GDA supports the functional and risk-based features of the draft Executive Order. The GDA also supports the recognition that certain government data can generally be stored and transferred outside of the Philippines as a default matter, but that – in relation to "secret" and "top secret" data – more rigorous controls are appropriate.

This functional and risk-based approach is preferable to broad and sweeping data localization mandates spanning an unduly wide array of data types. Unduly broad approaches risk undermining the Philippines' strategic goals in digital transformation, public health, and economic modernization – all of which depend upon cross-border access and sharing of knowledge, technical know-how, information, and other data types.

We support a functional, risk-based, and interoperable approach that upholds data classification and data security while promoting trusted and secure data mobility where appropriate. Such It rightly recognizes that cybersecurity, data security, and digital sovereignty are strengthened, not weakened, by responsible cross-border data exchange. We offer a few suggestions below:

1. Add a Preambular "Whereas" Recital that Recognizes the Benefits of Cross-Border Data Transfers

We observe that some of the "Whereas" recitals tend to focus on data-related risks, yet there is an absence of recitals focusing on the benefits of access to, and sharing of, data across borders. To promote a balanced and accurate perspective on these matters, we recommend the inclusion of an additional recital that recognizes the benefits of cross-border data transfers. The text of such a recital could – for example – read as follows:

> Whereas cross-border data flows support many public policy objectives of the Government of the Philippines relating to artificial intelligence, cyber-defense, digital transformation, economic opportunity, fraud prevention, health, privacy, safety, security, and regulatory compliance;

2. Add a Preambular "Whereas" Recital that Recognizes the Philippines' Support for Data Portability based on Principles of Accountability and Interoperability

The Philippines has long been a regional economic leader – in part due to its open, democratic, and forward-leaning strategic and economic posture. For example, the Philippines participates in a range of international initiatives that support cross-border data transfers. We recommend acknowledging those important accomplishments. The text of such a recital could – for example – read as follows:

> Whereas the Philippes is a strong supporter of the Global Cross-Border Privacy Rules Forum, as well as other initiatives in ASEAN, APEC, and the World Trade Organization focused on promoting responsible and seamless data transfers and freedom of choice in selecting data storage locations;

3. Add Text regarding the Default Presumption in favor of Responsible and Seamless Cross-Border Data Transfers

We would support a re-articulation of the principle outlined in the October 17 Circular published by DICT recognizing a default rule in favor of cross-border data transfers and against mandatory data residency. The text from the October 17 Circular could be adapted to the Executive Order as follows:

> "This Executive Order is grounded in a default presumption favoring cross-border data flows and freedom of choice in data storage determinations; however, in connection with certain data – such as data classified as "secret" and "top secret" – greater oversight and control is necessary."

Such a default norm that favors cross-border data mobility aligns with the GDA's Cross-Border Data Policy Principles,[2] and with good regulatory practices grounded in narrowly tailored regulations necessary to specific and legitimate public interest rationales, rather than blanket prohibitions.

4. Clarify the Treatment of "Confidential" Data

The discussion of "confidential" data would benefit from some clarification. Notably, paragraph one states unequivocally that such data must be stored within Philippine territory

(including embassies and consulates). However, paragraph two then states that "storage may be allowed offshore." The two concepts appear to be in conflict.

To avoid confusion, we would recommend revising the first paragraph as follows:

> All government data classified as "Confidential" " shall be stored in at least Tier III data center.... under the ANSI/TIA-942 standards, whether government owned or directly controlled infrastructure. [ADD: It is preferred to store such data] within Philippine territory, or in other territories over which the Philippines exercise such as, but not limited to, Philippine embassies and consulates.
>
> However, the storage of Confidential government data shall ~~may~~ be allowed offshore, provided that..."

To give regulated parties legal certainty, we also recommend changing "may" to "shall" in the second paragraph.

Finally, please recall the clear formulation from the DICT Oct. 17 circular:

> *"Government data classified as Sensitive, Confidential, and Open shall be permitted for storage and processing on secure cloud-computing platforms, irrespective of the physical location of the platform or ownership, subject to encryption, risk mitigation, and other cybersecurity requirements, and the fulfillment of compliance requirements prescribed by the DICT."*

This provision reflected a pragmatic, technology-neutral framework that strengthened security through operational safeguards rather than geographic mandates. It recognizes that security is a function of controls, not coordinates. It also was not overly prescriptive.

5. Recommendations for Data Transfer Provisions

As noted in comment 3 above, we recommend that the Executive Order reflect a default presumption in favor of responsible and seamless cross-border data transfers.[3] By maintaining this default openness—combined with targeted, risk-based safeguards—the Executive Order would reinforce the Philippines' position as an open, trusted, and sovereign digital economy, capable of safeguarding national interests while enabling growth and cross-border collaboration.

a. Adequacy, Contractual Mechanisms, and other Transfer Safeguards

We appreciate the reference at the bottom of Section 16 to "contractual clauses, binding corporate rules, or other safeguards." In implementing this provision, we encourage DICT to permit companies to leverage existing mechanisms, including ASEAN Model Contractual Clauses, the EU GDPR Standard Contractual Clauses, and equivalent mechanisms under OECD and APEC frameworks. We also encourage inclusion of an explicit reference to the Global Cross-Border Privacy Rules Forum, in which the Philippines participates. This interoperability will support legal certainty, regulatory compliance, and mutual recognition between the Philippines and its trading partners.

b. Encryption and Risk-Mitigation Protocols

We endorse the Executive Order's requirement for "state-of-the-art encryption protocols" and "documented risk mitigation strategies," while urging flexibility. Experience in other economies shows that overly prescriptive technical mandates can hinder innovation and paradoxically weaken security. For example, in certain other countries, overly restrictive

approaches have not enhanced cyber resilience. Rather, they have increased fragmentation, cost, and vulnerability.

The Philippines should avoid such rigidity by preserving technological neutrality and business flexibility within its cybersecurity rules. DICT should promote adaptive, outcomes-based cybersecurity—allowing regulated entities to demonstrate compliance through appropriate, risk-based measures suited to their circumstances.

c. Secret Government Data and Limited Processing Exceptions

We understand the Executive Order's interest in restricting cross-border processing of "Top Secret" or "Secret" government data. However, in some cases, this prohibition may unintentionally limit the ability to deploy secure AI tools and advanced analytics to such data in ways that could strengthen national defense and governance. Being able to apply AI and advanced analytics could – in some cases – be quite helpful to the Philippines, allowing limited cross-border processing where warranted for public safety, national defense, disaster response, or other limited purposes. These conditions could be elaborated in future technical guidance.

Thus, we welcome the inclusion of "cryptographic formats" as a means of permitting limited purpose transfers. We would also welcome the specification – either now or at a future date – of more specific details re the permissible transfer of such data for limited purposes.

6. Alignment with Allied Security Practices

We encourage the Philippines to continue to collaborate closely with the United States and other allies to share knowledge and learnings about data classification, "risk and impact assessments," "privacy impact assessments" and other new concepts in this measure. We also encourage more information sharing on best practices with industry.

Such alignment will facilitate cooperation and interoperability among trusted allies while strengthening the Philippines' own cyber and national security posture.

C. Conclusion

The draft Executive Order represents a major improvement over prior draft measures that sought to mandate data residency in the Philippines. The GDA stands ready to consult with or otherwise support the Government of the Philippines as it continues to develop these proposals.

---

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

[2] https://globaldataalliance.org/wp-content/uploads/2021/07/03022021gdacrossborderdatapolicyprinciples.pdf

[3] We encourage DICT to carefully review and benchmark the Executive Order 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.