GERONIMO
LAW

The U.S. CLOUD Act vs. Philippine Data Sovereignty

CONFLICT OF LAWS

PREPARED BY:
Russell Stanley Q. Geronimo
attorney@geronimo.law

FEBRUARY 28, 2026

GERONIMO LAW

6/F Valero One Center, Valero St., Salcedo Village, Makati City
www.geronimo.law
attorney@geronimo.law
+63 9999329836

The U.S. CLOUD Act vs. Philippine Data Sovereignty: Conflict of Laws

February 28, 2026

By Russell Stanley Q. Geronimo

Introduction

There is a risk of legal collision between the U.S. CLOUD[1] Act and Philippine government cloud data sovereignty rules.

On the one hand, the CLOUD Act mandates a location-agnostic disclosure obligation for U.S.-headquartered cloud providers. If the dataset is within a provider's "possession, custody, or control," a U.S. warrant can compel disclosure even when the data is stored abroad.

On the other hand, the Philippine Government Cloud First Policy stakes a strong sovereignty claim over government-linked cloud data "regardless of location," and it states that (except where Philippine law permits) such data shall not be "subject to foreign laws" or "accessible to other countries," regardless of the cloud model or provider nationality. The policy places strong residency restrictions on sensitive categories of government data.

CLOUD Act-Philippine law collisions may arise in scenarios where (a) a U.S.-headquartered provider offers cloud services to Philippine government entities or processes government-linked datasets, and (b) U.S. authorities serve U.S. legal process on that provider for data stored in the Philippines.

The CLOUD Act mandates disclosure compliance, while the Philippine Cloud First's data sovereignty policy mandates non-disclosure to foreign states and exclusion of foreign legal access. This presents a compliance dilemma for U.S.-headquartered providers.

Cloud Data Laws and Instruments

I. The CLOUD Act

The CLOUD Act has two pillars.

First, it clarifies that providers subject to U.S. jurisdiction must preserve and disclose covered communications and records within their "possession, custody, or control," regardless of whether the information is stored inside or outside the U.S.

Second, it authorizes bilateral executive agreements for cross-border data access (18 U.S.C. § 2523). These agreements are available only to rights-respecting partners meeting statutory requirements.

---

[1] "CLOUD" stands for Clarifying Lawful Overseas Use of Data.

For compelled content requests under the Stored Communications Act (SCA), 18 U.S.C. § 2703 includes a statutory mechanism for providers to move to modify or quash U.S. warrants on conflict-of-law grounds where the provider reasonably believes disclosure risks violating the laws of a "qualifying foreign government," and the subscriber is not a U.S. person and does not reside in the U.S. This is the exclusive statutory basis for quashing U.S. warrants on conflict-of-law grounds tied to qualifying foreign governments.

II. Philippine Government Cloud Data Sovereignty Rules

The Philippine Government Cloud First Policy is an instrument issued by the Department of Information and Communications Technology.

The 2017 Cloud First Department Circular states that GovCloud operations and related contracts and SLAs are governed by Philippine law and that disputes should be resolved in Philippine courts.

The 2020 amendment (Department Circular No. 010, Series of 2020) creates the core sovereignty conflict with the CLOUD Act clearly:

1. *Data sovereignty (Section 12.1)*

   Government-linked cloud data "regardless of location" is governed by Philippine laws and policies, and (except where otherwise permitted under Philippine law) shall not be subject to foreign laws or accessible to other countries, regardless of cloud deployment model, provider nationality, or storage location.

2. *Data residency (Section 12.2)*

   The circular states no general residency restrictions for government cloud data if controls exist, but places residency restrictions for sensitive, above-sensitive, and highly sensitive government data, including restrictions to Philippine territory or areas under Philippine sovereignty or jurisdiction and specified alternatives (including certain foreign states meeting listed conditions).

3. *Data ownership and encryption key control (Section 14.1)*

   The circular asserts Philippine government retention of "full control and ownership" and states, "to the exclusion of foreign governments," the Philippine government has the "sole authority" to determine management, use, processing, storage, security, and accessibility of its data, "with sole control over the encryption keys" subject to constitutional and legal requirements.

III. Bilateral and Multilateral Cooperation Instruments

The baseline bilateral channel for law enforcement evidence exchange is the Mutual Legal Assistance Treaty (MLAT)-based cooperation. The U.S.-Philippines MLAT provides a formal state-to-state path for evidence requests tied to criminal investigations and prosecutions.

Multilaterally, the Philippines is also a party to the Budapest Convention (Convention on Cybercrime) since 2018.

Conflict of Laws on Cloud Data

The CLOUD Act treats cloud evidence access as an extension of jurisdiction over the provider, while Philippine government-cloud sovereignty rules try to treat certain datasets as legally insulated from foreign jurisdiction regardless of physical location or provider nationality. This is a concrete compliance dilemma for cloud providers offering services to Philippine government entities or managing government-linked datasets in the Philippines, especially if the provider is also subject to a U.S. warrant.

A representative scenario may involve a U.S. warrant served on a U.S.-headquartered cloud provider for content stored in the provider's Philippines data center (or replicated there) tied to a Philippine government subscriber or a Philippine government ICT system. Under 18 U.S.C. § 2713, the provider's storage choice does not negate the disclosure duty if the provider has possession, custody, or control. The Philippine Cloud First data sovereignty clause, written to bind providers and intermediaries in government transactions, pushes in the opposite direction by purporting to exclude foreign legal access and foreign "accessibility."

Philippine Cloud First conditions are incorporated into government contracts, which gives agencies leverage through procurement enforcement and remedies, even when criminal enforcement against a foreign provider would be difficult.

Reconciliation mechanisms

The MLAT channel is the cleanest reconciliation mechanism because it expresses respect for territorial authority and domestic legal standards through a competent authority review and local execution route. This is true in both directions:

- For U.S. investigators seeking Philippine-located evidence, MLAT reduces the likelihood of a direct conflict with Philippine Cloud First sovereignty restrictions by moving the request into Philippine legal processes and judicial controls.
- For Philippine investigators seeking U.S.-held content, MLAT is often the lawful route absent a CLOUD Act executive agreement.

An executive agreement under § 2523 can also reduce conflict by establishing a mutually recognized legal lane where each state's orders can be served directly on providers in the other jurisdiction under defined limits.

For the Philippines, this option raises hard domestic questions because Philippine constitutional privacy protections emphasize lawful court order and inadmissibility of violations, and because Philippine policy (Cloud First) expresses a strong preference to exclude foreign government access for government-linked cloud data.

-end-