



MALACAÑAN PALACE  
MANILA

**EXECUTIVE ORDER NO. 119**

**UPDATING THE GOVERNMENT DATA CLASSIFICATION, ESTABLISHING A DATA RESIDENCY FRAMEWORK, AND FOR OTHER PURPOSES**

**WHEREAS**, Section 7, Article III of the Constitution recognizes the right of the people to information on matters of public concern, including access to official records, and to documents and papers on official acts, transactions, or decisions, as well as government research data used as basis for policy development, subject to limitations provided by law;

**WHEREAS**, Republic Act (RA) No. 10173 or the "Data Privacy Act of 2012" declares it a policy of the State to protect the fundamental human right to privacy of communication while ensuring free flow of information to promote innovation and growth;

**WHEREAS**, RA No. 10844 or the "Department of Information and Communications Technology (DICT) Act of 2015" mandates the DICT as the primary policy, planning, coordinating, implementing, and administrative entity of the Executive branch of the government that will plan, develop, and promote the national information and communications technology development agenda, including cybersecurity and data governance policies;

**WHEREAS**, Section 3, Chapter 2, Title VIII, Book IV of Executive Order No. 292 or the "Administrative Code of 1987" mandates the National Security Council (NSC) to serve as the lead agency of the government for coordinating the formulation of policies relating to or with implications on national security;

**WHEREAS**, Section 2 of RA No. 12254 or the "E-Governance Act" adopts a policy to establish, foster, and sustain a digitally empowered and integrated government through the implementation of a regulated and robust information and communication system aimed at facilitating responsive and transparent online citizen-centered services;

**WHEREAS**, Memorandum Circular (MC) No. 78 (s. 1964), as amended by MC No. 196 (s. 1968), established the data classification framework governing security of classified matter in government offices;

**WHEREAS**, the existing data classification framework established under MC No. 78, as amended, was formulated in the context of a paper-based bureaucracy and is no longer fully responsive to the demands of contemporary digital governance, cybersecurity risks, cloud computing environments, and cross-border data flows;

**WHEREAS**, there is a need to update and modernize the government's data classification structure and to establish a coherent policy framework on data residency

and cross-border data transfers to safeguard national security, uphold data sovereignty, ensure compliance with existing laws, and support secure digital transformation across government; and

**WHEREAS**, Section 17, Article VII of the Constitution vests in the President the power of control over all Executive departments, bureaus, and offices, and the mandate to ensure the faithful execution of laws;

**NOW, THEREFORE, I, FERDINAND R. MARCOS, JR.**, President of the Philippines, by virtue of the powers vested in me by the Constitution and existing laws, do hereby order:

**Section 1. Coverage.** This Order shall cover all government data in digital or hybrid form, owned, processed, or controlled by national government agencies and instrumentalities, including government-owned or -controlled corporations, and state universities and colleges, insofar as it is consistent with existing laws, rules, and regulations. The Legislature, Judiciary, Constitutional Commissions, Office of the Ombudsman, and local government units are hereby encouraged to adopt the provisions of this Order.

**Section 2. Applicability to Private Sector Data and Responsibility of Government Agencies.** This Order does not apply to the private sector or commercial data owned by private entities. However, this Order applies to government data or information processed or stored by private entities, including those engaged in public-private partnerships, public services, public utilities, critical infrastructure, or strategic or sensitive projects; on behalf of a government agency as may be defined in the implementing guidelines.

Government agencies that procure or utilize services from cloud service providers or other private entities for the storage or processing of government data remain responsible for ensuring data security and compliance with this Order. For this purpose, government agencies shall ensure the inclusion of appropriate contractual and technical safeguards to protect data handled by such service providers.

The routine collection or storage by private entities of copies of government-issued identification documents for legitimate business purposes shall not be considered government data for purposes of this Order.

**Section 3. Adoption of the Updated Government Data Classification Framework.** The Government Data Classification Framework established under MC No. 78 (s. 1964), as amended, is hereby updated in accordance with the provisions of this Order. All covered government entities shall adopt a unified, and risk-based framework for the classification, protection, handling, and management of government data.

**Section 4. Data Classification Framework.** Government data shall be classified into two (2) general classes: Restricted Access Data and Open Access Data, in accordance with the updated Government Data Classification Framework adopted under this Order.

- a. **Restricted Access Data** refers to official matters requiring protection in the interest of national security. Data classification shall take into account potential unauthorized disclosure to foreign governments or entities, which

could compromise diplomatic positions, intelligence operations, defense planning, and economic strategies. These shall be limited to four (4) categories of classification, which, in descending order of importance, shall carry one of the following designations:

- i) **Top Secret** refers to information or matters the unauthorized disclosure of which would cause exceptionally grave damage to the nation, politically, economically, or from a security aspect;
  - ii) **Secret** refers to information or matters the unauthorized disclosure of which would endanger national security, cause serious injury to the interest or prestige of the nation, or of any government activity, or would be of great advantage to a foreign nation;
  - iii) **Confidential** refers to information or matters the unauthorized disclosure of which, while not endangering the national security, would be prejudicial to the interest or prestige of the nation or any government activity, or would cause administrative embarrassment or unwarranted injury to an individual, or would be of advantage to a foreign nation; and
  - iv) **Restricted** refers to information or matters which require protection other than that determined to be Top Secret, Secret, or Confidential.
- b. **Open Access Data** refers to information or matters not falling within Restricted Access Data as defined in Section 4(a) hereof and does not involve national security. Such data may be designated as Unclassified or Open, subject to applicable laws, rules, and regulations.

**Section 5. Risk-based Methodology for Data Classification.** All covered government agencies shall adopt a risk-based methodology for data classification. The originating agency of government data shall be responsible for determining the appropriate classification of data under its custody based on an assessment of the potential harm that may arise from unauthorized disclosure, alteration, destruction, or misuse.

The risk-based methodology shall include, at a minimum:

- a. The identification and inventory of government data under the custody or control of the agency;
- b. The conduct of appropriate risk and impact assessments, including, where applicable, privacy impact assessments in accordance with existing laws;
- c. The application of classification levels commensurate with the highest assessed level of risk; and
- d. The continuing review of classified data, including downgrading or declassification when warranted.

All data classification, legal basis, and risk assessments shall be recorded in a Government Data Classification Registry System, to be developed and maintained by the DICT.

**Section 6. Prohibition on Overclassification.** Overclassification is prohibited to maintain the integrity of the data classification framework, ensure the importance of correctly classified data, and prevent unnecessary delay, expense, or administrative burden.

**Section 7. Data Residency Framework.** All government data shall remain subject to the laws and jurisdiction of the Republic of the Philippines, regardless of where such data is stored, processed, or handled.

In accordance with the Data Classification Framework established under Section 4 of this Order, all government data shall adhere to the following mandatory storage and residency requirements:

- a. Data classified as Top Secret and Secret shall be stored within Philippine territory or in other territories over which the Philippines exercises sovereignty or jurisdiction, such as, but not limited to, Philippine embassies and consulates;
- b. Data classified as Confidential shall, as a general rule, be stored and maintained within Philippine territory or in other territories over which the Philippines exercises sovereignty or jurisdiction, such as, but not limited to, Philippine embassies and consulates. By way of exception, such data may be stored or processed outside Philippine territories, provided that the responsible agency obtains the express prior approval of the Joint Oversight Committee for Data Classification (JOC-DC), and ensures the implementation of adequate safeguards that maintain governmental control and afford protection consistent with national security and applicable laws;
- c. Data classified as Restricted shall be permitted to be stored on a secured cloud computing platform subject to encryption, risk mitigation, and other cybersecurity requirements; and
- d. All other government data, including open access data, shall be permitted for storage on secure cloud-computing platforms, irrespective of the physical location of the platform or the ownership, subject to encryption, risk mitigation, and other cybersecurity requirements.

**Section 8. Cross-Border Data Transfers.** Cross-border transfers of government data may be undertaken in accordance with the Data Classification Framework established in this Order and the implementing guidelines.

Pursuant to the Principle of Accountability under Section 21 of RA No. 10173, cross-border data transfer of government data containing Personal Information or Sensitive Personal Information shall require that the Personal Information Controller guarantee a standard of protection comparable to that required by RA No. 10173.

**Section 9. Applicability of Information Security.** The principles of Communication Security under MC No. 196 are hereby expanded to cover all forms of digital information and communications, collectively referred to as Information Security. Information Security shall apply to all government data, whether in physical, digital, or

hybrid form, and shall be implemented in a manner commensurate with the classification of the data and consistent with national security and applicable laws.

Covered government agencies shall designate an information security officer responsible for the implementation of this Section. Such officer shall obtain and maintain the appropriate level of national security clearance, as may be required, in accordance with applicable laws, rules, and regulations.

**Section 10. Capacity Building, Training, and Knowledge Sharing.** The DICT, in collaboration with the National Privacy Commission (NPC), relevant government agencies, academic institutions, and industry partners, shall formulate and promulgate a comprehensive training and competency framework on data protection, residency, and cloud governance. The DICT shall finalize the training programs and publish the official training modules and curriculum within one hundred twenty (120) days from the effectivity of this Order.

**Section 11. Creation of Joint Oversight Committee for Data Classification.** To ensure the orderly and effective implementation of this Order, a JOC-DC is hereby created.

The JOC-DC shall be composed of the heads of the following agencies:

|                 |   |                                                                                                                                                                                                                          |
|-----------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Co-Chairpersons | : | DICT and NSC                                                                                                                                                                                                             |
| Members         | : | Department of the Interior and Local Government;<br>National Intelligence Coordinating Agency;<br>Department of Foreign Affairs;<br>NPC;<br>Philippine Statistics Authority; and<br>National Archives of the Philippines |

The DICT and NSC shall jointly serve as Secretariat of the JOC-DC, and shall provide administrative and technical support to the Committee. The Secretariat shall be headed by the DICT.

The Co-Chairpersons and members of the JOC-DC may designate their respective alternates, with ranks not lower than Assistant Secretary or its equivalent, who shall be fully authorized to decide for or on their behalf. The JOC-DC shall convene at least once every quarter or as often as may be deemed necessary by the Co-Chairpersons.

**Section 12. Duties and Functions of the JOC-DC.** The JOC-DC shall oversee the implementation of this Order and shall exercise the following duties and functions:

- a. Formulate and issue the implementing guidelines and related issuances necessary for the effective implementation of this Order, including, among others, the: (i) standards and procedures for classification of government data following a risk-based methodology as defined under Section 5 of this Order; (ii) policies on data residency and sovereignty frameworks; and (iii) procurement and utilization of a secure private cloud platform, subject to existing laws, rules, and regulations;

- b. Develop an action plan to be followed by all covered government agencies relevant to the compliance and implementation of this Order;
- c. Monitor and evaluate agency compliance with the Government Data Classification Framework;
- d. Submit annual reports to the President on the status of implementation and overall data governance compliance across government agencies;
- e. Conduct consultations with relevant government agencies and stakeholders to support the continuing development and refinement of policies under this Framework;
- f. Harmonize data classification practices across government and resolve inter-agency classification issues, consistent with the Philippine Government Interoperability Framework;
- g. Provide oversight over the Government Data Classification Registry System to ensure governance, security, and accountability. Such oversight shall be confined to policy-level supervision, compliance monitoring, and audit mechanisms, and shall not be construed as granting the JOC-DC or its members access to, or control over, the system or its underlying data, except as may be authorized under existing laws, rules, and regulations; and
- h. Call on other government agencies or, when necessary, private entities to assist the JOC-DC in the performance of its duties and functions.

The implementing guidelines shall be issued within one hundred twenty (120) days from the effectivity of this Order.

**Section 13. Monitoring and Reporting.** All government agencies and entities covered by this Order are hereby required to submit an annual report on their compliance to the JOC-DC. The JOC-DC shall submit to the President, through the Office of the Executive Secretary, an annual consolidated report on the implementation of this Order.

**Section 14. Administrative Liability.** Failure to comply with the provisions of this Order shall constitute a ground for administrative or disciplinary sanctions against any erring public official or employee, as provided under existing laws and regulations, without prejudice to criminal, civil, or other related liabilities under existing laws.

**Section 15. Transition and Phased Implementation.** Covered government agencies shall achieve full compliance with this Order within three (3) years from its effectivity. Implementation shall be undertaken in phases, subject to the following minimum milestones:

- a. **First Year.** Within the first year from the effectivity of this Order, covered government agencies shall complete capacity-building measures, conduct an inventory of government data, and undertake the initial classification of datasets and workloads.
- b. **Second Year.** Within the second year from the effectivity of this Order, covered government agencies shall ensure full compliance with the requirements of this Order for data classified as Top Secret and Secret.
- c. **Third Year.** Within the third year from the effectivity of this Order, covered government agencies shall ensure full compliance with the requirements of this Order for all remaining government data.

During the transition period, agencies may continue to utilize existing infrastructure and services, provided that they take reasonable measures to manage risks and ensure alignment with the objectives of this Order.

Nothing in this Section shall be construed to suspend or defer compliance with RA No. 10173 and other applicable laws. All government entities shall remain accountable for compliance with existing legal requirements throughout the transition period.

**Section 16. Funding.** The funding requirements for the initial implementation of this Order shall be charged against current and available appropriations of concerned agencies, subject to relevant budgeting, accounting, and auditing laws, rules, and regulations. Thereafter, the funding requirements necessary for the continued implementation of this Order shall be included in the budget proposals of concerned agencies, subject to the usual budget preparation process.

**Section 17. Separability.** If any section or part of this Order is declared unconstitutional or invalid, the other sections or provisions not otherwise affected shall remain in full force and effect.

**Section 18. Repeal.** All issuances, orders, rules, and regulations, or parts thereof, that are inconsistent with the provisions of this Order, are hereby repealed or modified accordingly.

**Section 19. Effectivity.** This Order shall take effect immediately upon publication in the Official Gazette or in a newspaper of general circulation.

**DONE**, in the City of Manila, this 13th day of July, in the year of our Lord, Two Thousand and Twenty-Six.



By the President:



**RALPH G. REGIO**  
Acting Executive Secretary

