Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Circular Year-NO.

Date : **XX Month XXXX**

Subject : **PREREQUISITES FOR THE PHILIPPINE PRIVACY MARK CERTIFICATION PROGRAM**

WHEREAS, Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications in nation-building and its inherent obligation to ensure that personal data in information and communications systems in the government and the private sector are secured and protected;

WHEREAS, pursuant to Section 7 of the DPA, the National Privacy Commission (NPC) is charged with the administration and implementation of the provisions of the law, which includes monitoring and ensuring compliance of the country with international standards set for data protection, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country, in coordination with other government agencies and the private sector;

WHEREAS, the National Privacy Commission (NPC) is developing the Philippine Privacy Mark (PPM) Certification Program, a voluntary certification program, to assess public and private organizations that implement data privacy and protection management systems, to ensure the secure and protected processing of personal information;

WHEREAS, the PPM Certification Program shall evaluate the processing activities of organizations and the implementation of proper data protection measures and policies through a management system. It will enable organizations to reduce risks and demonstrate compliance with the DPA, its IRR and other Commission's issuances, and data subjects to identify organizations they can trust with their personal data;

WHEREAS, organizations and Certification Bodies who wish to voluntarily participate in the PPM Certification Program shall comply with the pre-requisites for certification or accreditation;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Circular governing the pre-requisites for both organizations and Certification Bodies (CBs) who will participate in the PPM Certification Program.

SECTION 1. ***Scope.*** This Circular shall apply to all personal information controllers (PICs) or personal information processors (PIPs) that will seek certification under the PPM Certification

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Program, and to all Certification Bodies (CBs) that will seek accreditation under the PPM Certification Program.

SECTION 2. ***Purpose.*** This Circular provides the prerequisites for certification of PICs or PIPs and accreditation of CBs under the PPM Certification Program.

SECTION 3. ***Definition of Terms.*** The definition of terms in the DPA and its IRR, as amended, are adopted herein. In addition, whenever used in this Circular, the following terms are defined as follows:

A. "Accreditation" refers to a third-party attestation related to a conformity assessment body conveying a formal demonstration of its competence to carry out specific conformity assessment tasks.
B. "Certification" refers to a third-party attestation related to an object of conformity assessment (e.g., product, process, service, system, installation, project, data, design, material, claim, person, body, or organization) with the exception of accreditation.
C. "Certification Body (CB)" refers to a third-party conformity assessment body;
D. "International Electrotechnical Commission (IEC)" refers to an organization that prepares and publishes international standards for all electrical, electronic and related technologies;
E. "International Organization for Standardization (ISO)" refers to an independent, non-governmental international organization with a membership of one hundred sixty-seven (167) national standards bodies that share knowledge and develop voluntary, consensus-based, and market relevant international standards that support innovation and provide solutions to global challenges;

SECTION 4. ***Requirements for PIC or PIP***. Prior to applying for certification under the PPM Certification Program, a PIC or PIP must be certified with the following standards:

I. ISO/IEC 27001 - information security management system (ISMS): specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization; and
II. ISO/IEC 27701 – privacy information management system (PIMS): specifies the requirements and guides for establishing, implementing, maintaining, and continually improving a PIMS in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 (which provides a reference set of generic information security controls including implementation guidance) for privacy management within the context of the organization.

SECTION 5. ***Requirements for CB***. Prior to applying for accreditation under the PPM Certification Program, a CB must be certified with the following standards:

I. ISO/IEC 27001 - information security management system (ISMS): specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization;
II. ISO/IEC 27701 – privacy information management system (PIMS): specifies the requirements and guides for establishing, implementing, maintaining, and continually improving a PIMS in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 (which provides a reference set of generic information security controls including

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

implementation guidance) for privacy management within the context of the organization; and

III. ISO/IEC 17021-1: Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements.

A CB shall complete the following accreditation stages:

I. Stage 1: Obtained a foreign or local accreditation to conduct audit or conformity assessment against the ISO/IEC 27001 standard;
II. Stage 2: Obtained a foreign or local accreditation to conduct audit or conformity assessment against the ISO/IEC 27701 standard; and
III. Stage 3: Obtained accreditation to conduct audit or conformity assessment against the PPM Certification Program.

SECTION 6. ***Failure to Comply***. A PIC or PIP and CB that fails to comply with the pre-requisites for certification or accreditation stated in this Circular shall not be qualified to apply for certification and accreditation under the PPM Certification Program, respectively.

ADDITIONAL MISCELLANEOUS PROVISIONS

SECTION 7. ***Amendments***. These Rules shall be subject to regular review by the Commission. Any amendment thereto shall be subject to the necessary consultations with the concerned stakeholders.

SECTION 8. ***Separability Clause***. If any portion or provision of these Rules is declared null and void or unconstitutional, then the other provisions not affected thereby shall continue to be in force and effect.

SECTION 9. ***Effectivity***. These Rules shall take effect immediately after publication in one newspaper of general circulation.

Approved:

JOHN HENRY D. NAGA
Privacy Commissioner

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NERISSA N. DE JESUS-LAZARO
Deputy Privacy Commissioner

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228