NPC Circular Year-NO.

Date : **XX Month XXXX**

Subject : **Certification Scheme – Part I - Requirements for Certification Bodies for the application and audit process of 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 NPC established 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 NPC issued NPC Circular 2023-05 which governs the pre-requisites for certification of personal information controllers (PICs) or personal information processors (PIPs) and accreditation of certification bodies (CBs) under the PPM Certification Program;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Circular governing the requirements for CBs for the application and audit process of the PPM Certification Program.

SECTION 1. ***Scope***. – This Circular specifies the requirements and provides guidance for bodies providing audit and certification of a Data Privacy and Protection Management System (DPPMS) and the competence requirements in providing certification assessment for the PPM Certification Program as well as the obligations of the accredited CBs.

SECTION 2. ***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. *"Audit"* refers to a systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled;
B. *"Accreditation"* refers to third party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks;
C. *"Accreditation Body (AB)"* refers to a wholly or partially automated processing operation that serves as the sole basis for making decisions that would significantly affect a data subject. It includes the process of profiling based on an individual's economic situation, political or religious beliefs, behavioral or marketing activities, electronic communication data, location data, and financial data, among others;
D. *"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;
E. *"Certification body"* refers to an organization that has been accredited to evaluate Personal Information Controllers and Processors against the PPM criteria, and to confer the PPM accordingly;
F. *"Data Privacy and Protection Management System (DPPMS)"* refers to the management system criteria that combine the elements of a Privacy Information Management System (PIMS), the DPA, and relevant issuances of the NPC.
G. *"Data processing system"* refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;
H. *"Evaluation"* refers to a systematic process of determining how the data privacy and protection management system has met the PPM Certification Program criteria;
I. *"Filing system"* refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;
J. *"Information and Communication Technology (ICT)"* refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document;
K. *"Information Security Management System (ISMS)"* refers to a the management system based on the ISO/IEC 27001 standard that uses a risk-based approach to establish, implement, operate, monitor, review, maintain, and improve information security.
L. *"Management system consultancy"* refers to participation in establishing, implementing or maintaining a management system

EXAMPLE 1:

Preparing or producing manuals or procedures.

EXAMPLE 2:

Giving specific advice, instructions or solutions towards the development and implementation of a management system.

Note 1 to entry: Arranging training and participating as a trainer is not considered consultancy, provided that, where the course relates to management systems or auditing, it is confined to the provision of generic information; i.e., the trainer should not provide client-specific solutions.

Note 2 to entry: The provision of generic information, but not client specific solutions for the improvement of processes or systems, is not considered to be consultancy. Such information may include: — explaining the meaning and intention of certification criteria; — identifying improvement opportunities; — explaining associated theories, methodologies, techniques or tools; — sharing non-confidential information on related best practices; — other management aspects that are not covered by the management system being audited.

M. *"Privacy Information Management System (PIMS)"* refers to a management system based on the ISO/IEC 27701 standard that addresses the protection of privacy as potentially affected by the processing of personal information;
N. *"Privacy risk"* refers to the potential effect of an uncertainty or an incident that may result in harm or danger to a data subject or an organization;
O. *"Recertification"* refers to the procedure for revalidation of a certificate by examination or by otherwise satisfying the certification body that the published criteria for recertification are satisfied;
P. *"Revocation"* refers to the process which revokes the authorization of an organization of its PPTM certification's validity;
Q. *"Surveillance"* refers to systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity;
R. *"Suspension"* refers to temporary removal or withholding of the certification due to non-conformance to the requirements or upon the occurrence of data breach;
S. *"Withdrawal"* refers to the removal of the certification or accreditation granted to the organization or certifying body, respectively.

SECTION 3. ***Eligibility***. – CBs who are interested in being accredited CBs for the PPM Certification Program shall need to comply with the NPC Circular No. 2023-05 and the following requirements:

A. Qualifications

1. Be an entity based in the Philippines (duly registered with SEC);
2. Have prior and ongoing experience in assessing and certifying entities of their management systems (e.g., quality management system, occupational and health safety, service management system, information security management system, among others); and
3. Have been accredited by a foreign or local accreditation body in auditing information security management systems or any relevant management system.

B. Competence - The CBs shall have relevant experience, training, activities, and pertinent certifications in the following disciplines:

a. Information security management systems (based on ISO/IEC 27001);
b. Privacy information management systems (based on ISO/IEC 27701);
c. Data privacy and data protection (including extensive knowledge on the DPA, its IRR, and issuances of the NPC through demonstration of CBs' compliance to DPA e.g., registered DPO/DPS, etc.

d. Technical knowledge of the activities to be audited;
e. Systems management or quality management;
f. Principles of auditing and impartiality (requirements in ISO/IEC 27006);
g. DPPMS monitoring, measurement, analysis, evaluation, and improvement;
h. Knowledge and experience in complaints, prohibited acts and appeals handling; and
i. Other relevant standards for data protection or guidelines for management systems (i.e., ISO/IEC 27001, ISO/IEC 27701, among others).

The CB's audit team shall have appropriate work experience and practical application in the above disciplines.

SECTION 4. ***Accreditation Recognition Process***. –The NPC shall recognize applicant CBs who are already accredited through local or international accreditation bodies to conduct certification and conformity assessments for the ISO/IEC 27001, 27701 and 17021-1. To be recognized, CBs shall submit the following documents in relation to Section 3 of this Circular.

A. **Eligibility Requirements. -** To be eligible for recognition under the PPM Certification Program, a CB must:

1. Be legally constituted and accredited as a CB in its country of origin;
2. Hold a valid accreditation for ISO/IEC 27001 (ISMS) and ISO/IEC 27701 (PIMS) certifications from a national accreditation body that is a signatory to the International Accreditation Forum (IAF) Multilateral Recognition Arrangement (MLA) or Asia Pacific Accreditation Cooperation (APAC) Mutual Recognition Arrangement (MRA);
3. Have at least a 3-year experience in conducting ISMS and PIMS certification audits;
4. Not have been the subject of any enforcement action or data breach investigation by the NPC in the last 2 years.

B. Application for Recognition. – Interested and eligible CBs shall submit the following to the NPC:

1. Accomplished Application Form for Recognition;
2. Certificate of No Pending Case issued by the NPC;
3. Copy of the certificate of the legal constitution in the country of origin;
4. Copy of valid ISO/IEC 27001 and ISO/IEC 27701 accreditation certificates;
5. Documentation of audit experience (e.g. number of clients certified per year);
6. Designation letter for the Philippine office or representative to handle PPM-related matters with contact details; and
7. Notarized undertaking to abide by the PPM Certification Scheme rules and requirements.

C. **Issuance of Certificate of Recognition. -** Upon determination by the NPC that the applicant CB has complied with all eligibility requirements and submitted complete documentation, it shall issue a Certificate of Recognition valid for 3 years.

The recognized CB will be listed in the registry of PPM certification bodies on the NPC website.

D. Validity and Renewal of Recognition. - The accreditation recognition shall be valid for 3 years from date of issuance, subject to the following conditions:

1. Continued compliance with eligibility requirements;
2. Timely submission of annual reports to the NPC;
3. No violations of PPM Certification Scheme rules and requirements; and
4. Uninterrupted validity of ISO 27001 and ISO 27701 accreditations.

E. Suspension and Termination of Recognition. - The NPC may suspend or terminate the accreditation recognition of a CB on any of these grounds:

1. Failure to maintain eligibility requirements;
2. Expiration, suspension or withdrawal of ISO/IEC accreditations;
3. Violations of PPM Certification Scheme rules and requirements;
4. Issuance of certifications in a fraudulent manner;
5. Closure of Philippine office or revocation of representative's designation; and
6. Upon request of the recognized CB.

The NPC shall notify the recognized CBs of suspension or termination. The suspension period would not exceed six (6) months. A suspended CB must rectify the deficiencies within a period prescribed by the NPC. Failure to do so shall result in termination of recognition. A terminated CB must undergo the full application process to regain recognition.

SECTION 6. ***Obligations of Recognized CBs*** - The accredited CBs that are recognized by the NPC can officially conduct PPM certification audits and renew the certification of organizations.

A. Appeals Handling

i. Establish a documented process to receive, evaluate and decide on appeals from applicant organizations regarding certification decisions;
ii. Ensure personnel handling appeals are different from those involved in the certification process;
iii. Include appeal decisions in the report to the NPC; and
iv. Comply with ISO/IEC 17021-1 requirements.

B. Managing Prohibited acts

1. Identify and manage potentially prohibited acts by certified organizations; and
2. Establish procedures and sanctions for violations of PPM usage rules and CB agreements.

C. Complaints Handling

1. Take responsibility for all actions and decisions in the complaints handling process;
2. Establish documented procedures and communication channels for client complaints;
3. Include complaint decisions in the report to the NPC; and
4. Comply with ISO/IEC 17021-1 requirements.

The Certification Scheme of the PPM Certification Program for applicant organizations shall be on a separate issuance of the NPC.

SECTION 7. ***Audit Process*** **–** Recognized accredited CBs shall carry out the following when auditing an applicant organization's Data Privacy and Protection Management System (DPPMS) for PPM Certification Program:

A. **General audit preparations**

1. Require applicant to provide access to internal audit reports and independent reviews of data privacy and protection (covering desktop and on-site assessment)
2. Obtain from applicant organization before the audit:

i. General documentation on DPPMS scope and covered processes; and
ii. Required DPPMS documentation specified in PPM requirements.

B. **DPPMS Scope**

1. Confirm the audit covers all aspects of the applicant's DPPMS based on PPM Certification Program requirements;
2. Check applicant's DPPMS Scope, Statement of Applicability, Privacy Impact Assessment (PIA), risk treatments and Privacy Management Program (PMP) reflect all processing activities; and
3. Ensure internal and external services integrated with DPPMS processes are documented and included in PIAs.

C. **Certification Audit Criteria**

i. **Governance:** purpose, roles, DPO designation, DPPMS scope, NPC registration;
ii. **Data Privacy Risk Management:** PIA, privacy engineering;
iii. **Operational Implementation:** PMP, PIAs, privacy manual/notices, processes; and
iv. **Continuous Improvement:** internal audits, surveillance, conformance checks.

The Data Privacy and Protection Management System (DPPMS) criteria of the PPM Certification Program for applicant organizations to comply and for CBs to audit against shall be on a separate issuance of the NPC.

Approved:

JOHN HENRY D. NAGA
Privacy Commissioner

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NERISSA N. DE JESUS
Deputy Privacy Commissioner