Republic of the Philippines
NATIONAL PRIVACY COMMISSION

DATA SECURITY AND COMPLIANCE OFFICE
Data Security and Technology Standards Division

ADVISORY ON THE ADOPTION OF INTERNATIONAL DATA PROTECTION STANDARD
NO. 2021-004
ISO/IEC 29134 – Information technology – Security techniques – Guidelines for privacy impact assessment

WHEREAS, Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012, 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 also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected;

WHEREAS, pursuant to Section 7 of the Data Privacy Act of 2012, the National Privacy Commission is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance by personal information controllers with the provisions of the Act and with international standards 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, Section 9 of the Implementing Rules and Regulations of the Data Privacy Act of 2012 provides that, among the Commission's functions, is to issue guidelines for organizational, physical and technical security measures for personal data protection, taking into account the nature of the personal data to be protected, the risks presented by the processing, the size of the organization and complexity of its operations, current data privacy best practices, cost of security implementation, and the most appropriate standard recognized by the information and communications technology industry, as may be necessary;

WHEREFORE, in consideration of these premises, the National Privacy Commission hereby issues this advisory on the adoption of ISO/IEC 29184 in conducting privacy impact assessments.

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Scope of the International Standard (IS)[1]

This document gives guidelines for:

- A process on privacy impact assessments (PIA), and
- A structure and content of a PIA report.

It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations.

This document is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process Personally Identifiable Information (PII).

Requirements

The IS provides guidelines for organizations in conducting PIA, the following are key points provided in the document:

- Preparation of the PIA
- Perform the PIA
- Follow up the PIA
- Structure of a PIA Report

Benefits

The following are key benefits of applying the IS within their organization:

- It provides clear guidance in conducting PIA which aligns with international best practices. It includes informative annexes like scale criteria for analyzing risk, generic threats, and examples of workflow diagram and risk map.
- Conducting PIA allows the organizations to identify potential privacy issues and risks on their processes, systems, or programs which is vital in avoiding costly and damaging privacy mistakes and possible legal consequences.
- PIA demonstrates the organization's commitment to respecting the data subjects' privacy and more likely to build their trust.

Guide for Adoption

PIA is a new type of risk assessment for most of the organizations here in the Philippines. It hasn't been a well-known practice for organizations to conduct PIA until the enactment of RA

[1] https://www.iso.org/standard/62289.html
The scope is directly lifted from the IS document, terms may be different from the DPA of 2012 but it has the similar meaning to the DPA terms. Refer to Annex A for the comparison of terms.

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

10173, also known as the Data Privacy Act of 2012 (DPA). Hence, the IS provides helpful guidance for organizations on how to conduct PIA. The IS has been adopted as a Philippine National Standard (PNS) by the Department of Trade and Industry – Bureau of Philippine Standards – Technical Committee 60 (DTI-BPS-TC60). The technical committee is in charge of reviewing and adopting any relevant international standards that will be distributed in the Philippines. This IS can be a supplemental guidance with the NPC Advisory 17-03 – Guidelines on Privacy Impact Assessment. Annex B illustrates the similarities of the advisory with the IS.

Personal Information Controllers (PICs) and Personal Information Processors (PIPs) who will adopt this IS within their organizations shall still comply with provisions of the DPA, its IRR, and other relevant issuances of the National Privacy Commission (NPC). The guidance for comparing the terms in Annex A. The IS does not amend the DPA, its IRR, and other relevant issuances of the NPC. In the event of a conflict between the provisions of the IS and the compliance requirements stated in the DPA, its IRR, and other relevant issuances of the NPC, the latter shall prevail.

The copy of the standards is available for a minimal fee at the Standards Data Center of the BPS – 3F DTI Bldg., 361 Sen. Gil Puyat Ave., Makati City. For quotation, please email BPS at bps@dti.gov.ph.

Prepared By:

Digitally signed by Aragona Shaira Valle

SHAIRA V. ARAGONA
ISA II, DSTSD

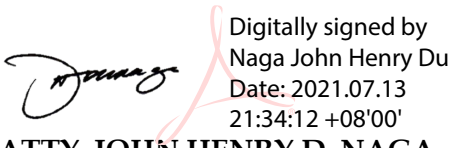
Reviewed By

Digitally signed by Magtalas Kelvin Santos
Date: 2021.07.09 13:53:11 +08'00'

KELVIN S. MAGTALAS
OIC-Chief, DSTSD

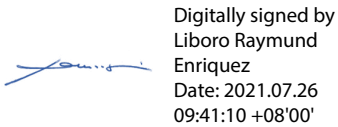
5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Recommending Approval:



ATTY. JOHN HENRY D. NAGA
OIC-Director, DASCO

Approved By:



RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Annex A – DPA and ISO/IEC 29100 Terms and definitions

	DPA of 2012	ISO/IEC 29100
Term	**Personal information**	**Personally Identifiable Information (PII)**
Definition	Refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.	any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal
Term	**Personal Information Controller (PIC)**	**PII Controller**
Definition	refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes: 1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or 2. A natural person who processes personal data in connection with his or her personal, family, or household affairs; There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing; privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes	privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes
Term	**Personal Information Processor (PIP)**	**PII processor**

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Definition	refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject	privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller
Term	**Data Subject**	**PII Principal**
Definition	refers to an individual whose personal, sensitive personal, or privileged information is processed	natural person to whom the personally identifiable information (PII) relates. *Note: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal"*
Term	**Personal Data Breach**	**Privacy breach**
Definition	refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach maybe in the nature of: 1. An availability breach resulting from loss, accidental or unlawful destruction of personal data; 2. Integrity breach resulting from alteration of personal data; and/or 3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.	situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements
Term	**Sensitive Personal Information (SPI)**	**Sensitive PII**
Definition	refers to personal information: 1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; 2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings; 3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous	category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal *Note: In some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that might be defined as sensitive.*

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

	or current health records, licenses or its denials, suspension or revocation, and tax returns; and 4. Specifically established by an executive order or an act of Congress to be kept classified.	
Term	**processing**	**processing of PII**
Definition	refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data;	operation or set of operations performed upon personally identifiable information (PII) *Note: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.*
Term	**third party**	**third party**
Definition	*Mentioned but nit defined*	privacy stakeholder other than the personally identifiable information (PII) principal, the PII controller and the PII processor, and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor
Term	**consent**	**consent**
Definition	refers to any freely given, specific, informed indication of will, hereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.	PII principal's freely given, specific and informed agreement to the processing of their PII

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Annex B –ISO/IEC 29134 and NPC Advisory 17-03 Matrix

This table is the matrix of the correlation of the NPC Advisory 17-03 with the ISO/IEC 29134.

ISO/IEC 29134	NPC Advisory 17-03
Clause 6	General Principles
Clause 5.1	Key Considerations
Clause 5.2	Objectives
Clause 5.3	Responsibility
Clause 6.3.4	Stakeholder Involvement
Clause 7	Structure and Form
Clause 6.1, 6.2	Planning a PIA
Clause 6.3	Preparatory Activities
Clause 6.4	Conduct of PIA
Clause 7	Documentation and Review
Clause 5.3	Compliance and Accountability

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph