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. 2021-001
ISO/IEC 29100 – Information technology – Security techniques – Privacy framework

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 29100 in implementing the framework in any information and communication technology (ICT) systems or services where privacy controls are required for personal data processing.

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 IS provides a privacy framework which:

- specifies a common privacy terminology;
- defines the actors and their roles in processing personally identifiable information (PII);
- describes privacy safeguarding considerations; and
- provides references to known privacy principles for information technology.

This IS is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering and operating information and communication technology (ICT) systems or services where privacy controls are required for processing PII.

Requirements

Personal information controllers (PICs) and personal information processors (PIPs) may choose to apply the requirements stated in this IS to further protect the personal data they handle or process on top of their compliance with the DPA.

Risk Management

PICs and PIPs perform broad risk management activities and develop risk profiles or criteria related to their ICT systems in order to manage threats, vulnerabilities and risks that accompany the processing of personal data. The IS provides a general framework regarding the following factors:

- Legal and regulatory factors
- Contractual factors
- Business factors
- Other factors (privacy preferences of PII Principals, internal controls and technical standards)

Privacy policies

PICs and PIPs involved in the processing of any kind of personal data should establish a privacy policy. The IS provides guidance on what the policy should contain and its relationship with a privacy notice, which is required at all points of personal data collection under the principles of openness, transparency and notice.

Privacy controls

Controls are essential in data privacy in keeping the personal data protected. This IS provides general guidance on how they will become an integral part of an organization's information security framework.

[1] https://www.iso.org/standard/45123.html

The scope is from the IS document itself. Terms may be different from those in the Data Privacy Act of 2012 but they have the similar meanings.

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

Privacy Principles
The privacy principles described in this standard were derived from existing principles developed by a number of states, countries and international organizations. Hence, this framework is a representation of privacy principles across the globe.

The following principles are further explained in the IS:

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

Benefits

The key benefits to PICs and PIPs applying the IS within their organizations are as follows:

- The IS can serve as basis for existing and new privacy standardization initiatives, e.g., as a technical reference architecture when designing ICT systems, the use of specific privacy technologies, a privacy management program, privacy impact assessments, and engineering terms.
- It can help both data subjects and organizations define privacy safeguarding requirements as they relate to all personal data and ICT systems.
- It is applicable on a wide scale – it sets a common privacy terminology, defines extensive privacy principles when processing personal data, classifies privacy features, and relates all described privacy aspects to existing security guidelines.
- It can be linked to existing security standards that have been put into practice worldwide.
- It helps identify organizational, technical, procedural and regulatory requirements and puts them into perspective and address system-specific matters on a high-level framework.
- It provides guidance relating to ICT requirements for processing personal data to ensure privacy on an international level.

Guide for Adoption

The ISO/IEC 29100 – Privacy framework is a very useful document for organizations willing to apply internationally recognized controls on their ICT systems. This IS was approved for adoption as a Philippine National Standard (PNS) by the Bureau of Philippine Standards upon the recommendation of the Subcommittee on Information security, cybersecurity and privacy

protection (SC 1) and the Technical Committee on Information Technology (BPS/TC 60). BPS/TC 60 is in charge of the review and adoption of relevant international standards that will be distributed in the Philippines.

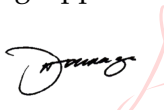
PICs and PIPs which will apply this IS within their organizations shall still follow the terminologies in the DPA, its IRR and other relevant issuances of the National Privacy Commission (NPC). Guidance on the comparison of terms is in Annex A. The IS does not amend the DPA, its IRR, and other relevant 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.

A copy of the standard 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:

KELVIN S. MAGTALAS
OIC-Chief, DSTSD

Recommending Approval:



JOHN HENRY D. NAGA
OIC-Director, DASCO

Approved By:

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

ANNEX A – DPA and ISO/IEC Terms and Definition

	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
Term	**Personal Information Processor (PIP)**	**PII Processor**
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

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

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 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.	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.*
Term	**Processing**	**Processing of 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

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 not 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 of the Data Subject**	**Consent**
Definition	Refers to any freely given, specific, informed indication of will, whereby 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 – Data Privacy Principles Matrix

ISO/IEC 29100	DPA of 2012				
	Transparency	**Legitimate Purpose**	**Proportionality**	**Rights of the Data Subjects**	**Obligations of PIC/PIP**
Consent and choice	✓				
Purpose legitimacy and specification		✓			
Collection limitation			✓		
Data minimization			✓		
Use, retention and disclosure limitation			✓		
Accuracy and quality			✓		
Openness, transparency and notice	✓				
Individual participation and access	✓	✓		✓	
Accountability		✓			✓
Information security		✓			✓
Privacy compliance		✓			✓

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