

ATTY. AMOR G.
VENENOSO

COMPLIANCE AND
MONITORING
DIVISION

Data Privacy Act of 2012

2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020

2019 *This Is What Happens In An* Internet Minute

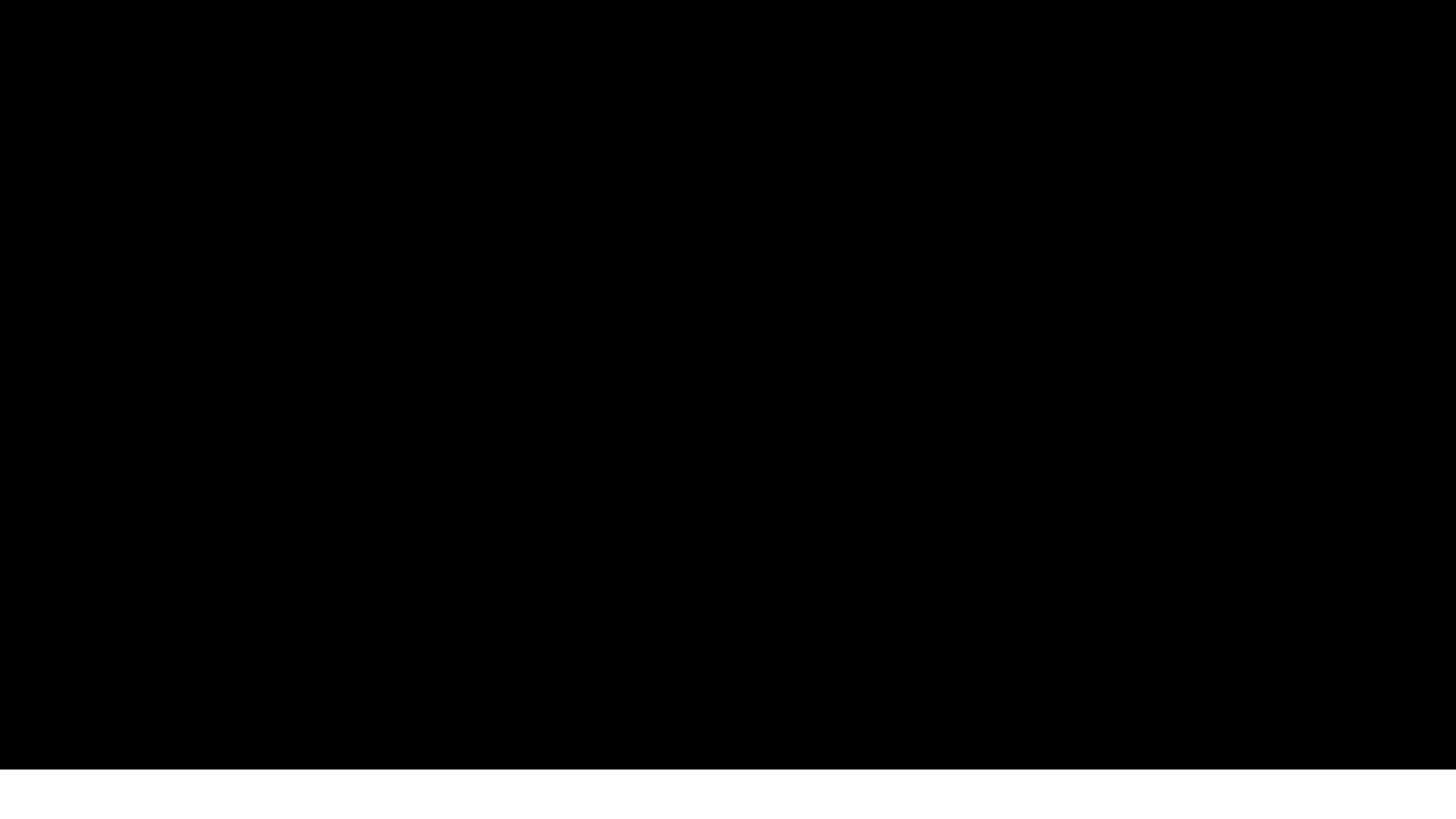


2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020

Created By:
[@LoriLewis](#)
[@OfficiallyChadd](#)

How important is your personal data?

2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020





Facebook breach affects 755,000 accounts in PH

Facebook Loses Around \$13 Billion in Value After Data Breach Affects 50 Million of Its Users

TECH NEWS

171,000 Filipinos affected by Uber data breach

Uber says exposed were the phone numbers, email addresses

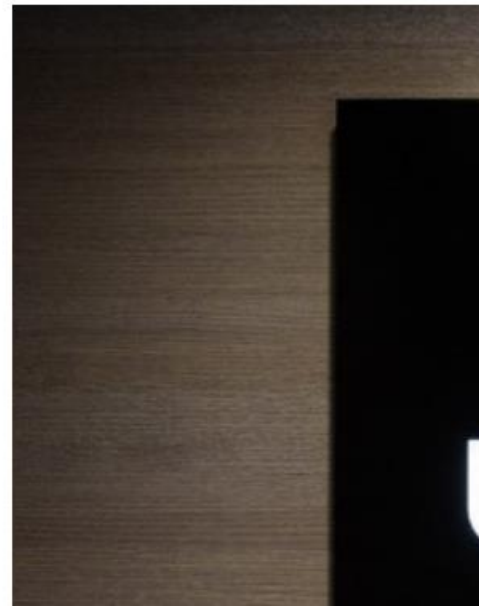
Gelo Gonzales
Published 11:55 AM, December 15, 2017
Updated 12:13 PM, December 15, 2017

Facebook

Twitter

Reddit

Email



By **KEVIN KELLEHER** September 28, 2018

2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020

2018 continues to be a challenging year for **Facebook**. The company's stock closed down 3% Friday following **reports** that hackers gained access to the personal data on 50 million of its users.

Identity Theft



Access to personal information such as name, date of birth, address, or email address can result to fraudsters victimizing individuals.

2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020



1004



30



2



0



Public school teacher in debt because of identity theft

Published February 26, 2016 10:48pm

A public school teacher may be a victim of identity theft as he owes three banks P800,000 for loans he did not apply for, according to a report by John Consulta on GMA-7's "24 Oras" on Friday.

~~Mark Joseph Lantok~~ said he received notifications from three banks saying that he borrowed a total of P800,000 in salary loans. He denied applying for the loans.

However, ~~Lantok~~ remembered posting a photo of his Professional Regulation Commission (PRC) ID online.

“Yong time na nakapasa ako sa LET (License Examination for Teachers), nag-post ko sa Facebook ako. Tsaka pagpasok ko po sa public (school), pagbigay ng papel ko, pinost din sa Facebook (Facebook) sa sobrang tuwa ko po,” he said.

“Wala naman akong ginagawang masama,” he added.

Data Privacy Act of 2012

REPUBLIC ACT 10173


2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020



The Data Privacy Act makes it mandatory for all data collectors — whether public or private — to protect the security, integrity and confidentiality of all the personal information they collect. **By doing this, we help usher in a truly knowledge-driven economy.**

2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020

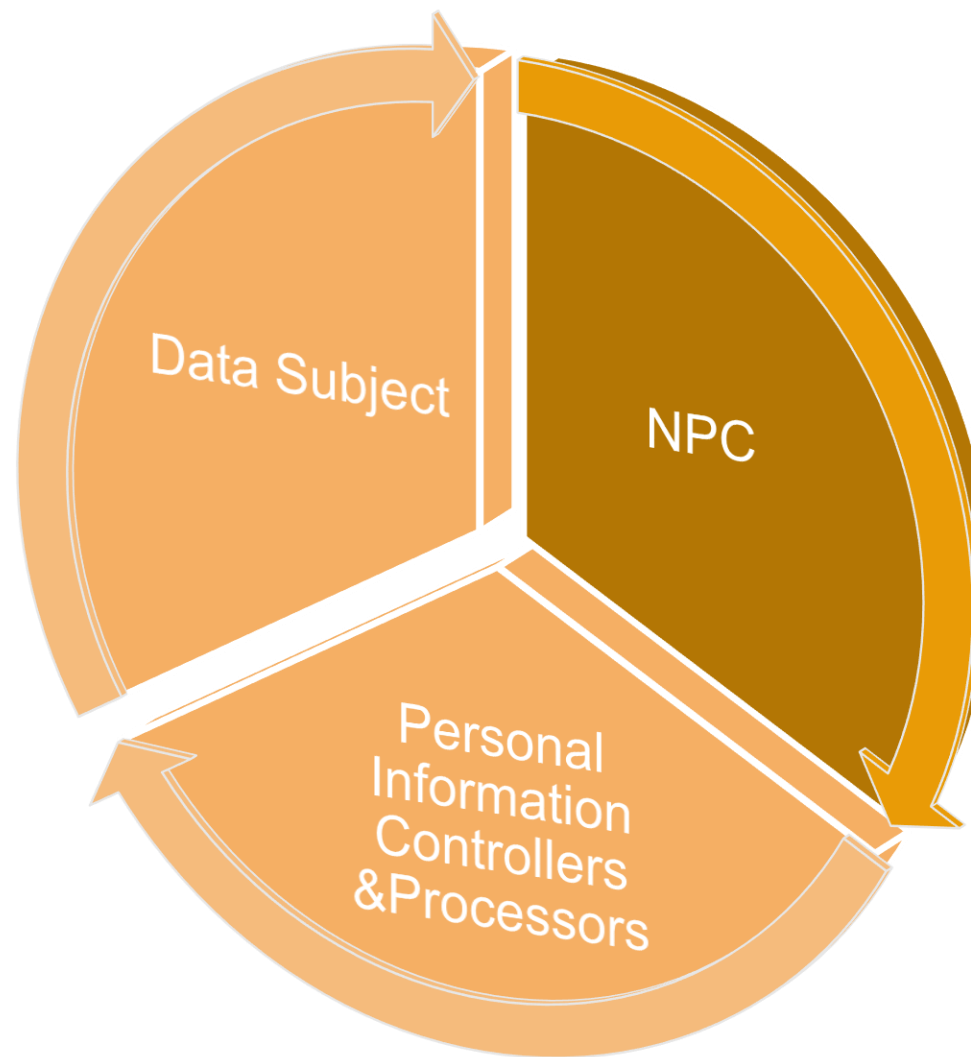
SENATOR EDGARDO ANGARA

- 
- ▶ The law upholds the right to privacy by protecting **individual personal information**.
 - ▶ The National Privacy Commission protects individual personal information by **regulating the processing** of personal information.

Scope of the DPA

- ▶ Applies to the processing of **all types of personal information**, in the **country** and even **abroad**, subject to certain qualifications. (Section 4)

The Privacy Ecosystem



PERSONAL INFORMATION

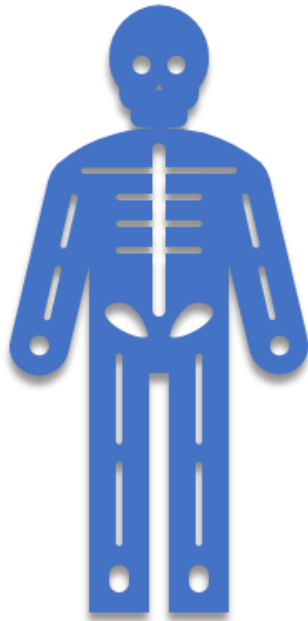


Any information whether recorded in a material form or not, from which the **identity of an individual is apparent or can be reasonably and directly ascertained** by the entity holding the information, or when **put together with other information would directly and certainly identify an individual.**

It includes

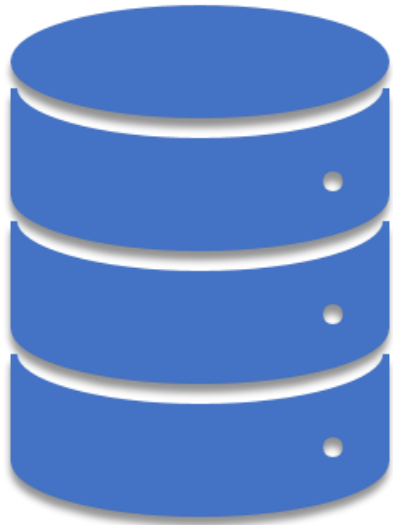
- ▶ Full name
- ▶ Passport number
- ▶ Vehicle license plate number
- ▶ Photograph / Video images of an individual
- ▶ Mobile telephone number
- ▶ Personal email address
- ▶ Thumbprint
- ▶ DNA profile
- ▶ residential address
- ▶ residential telephone number

SENSITIVE PERSONAL INFORMATION

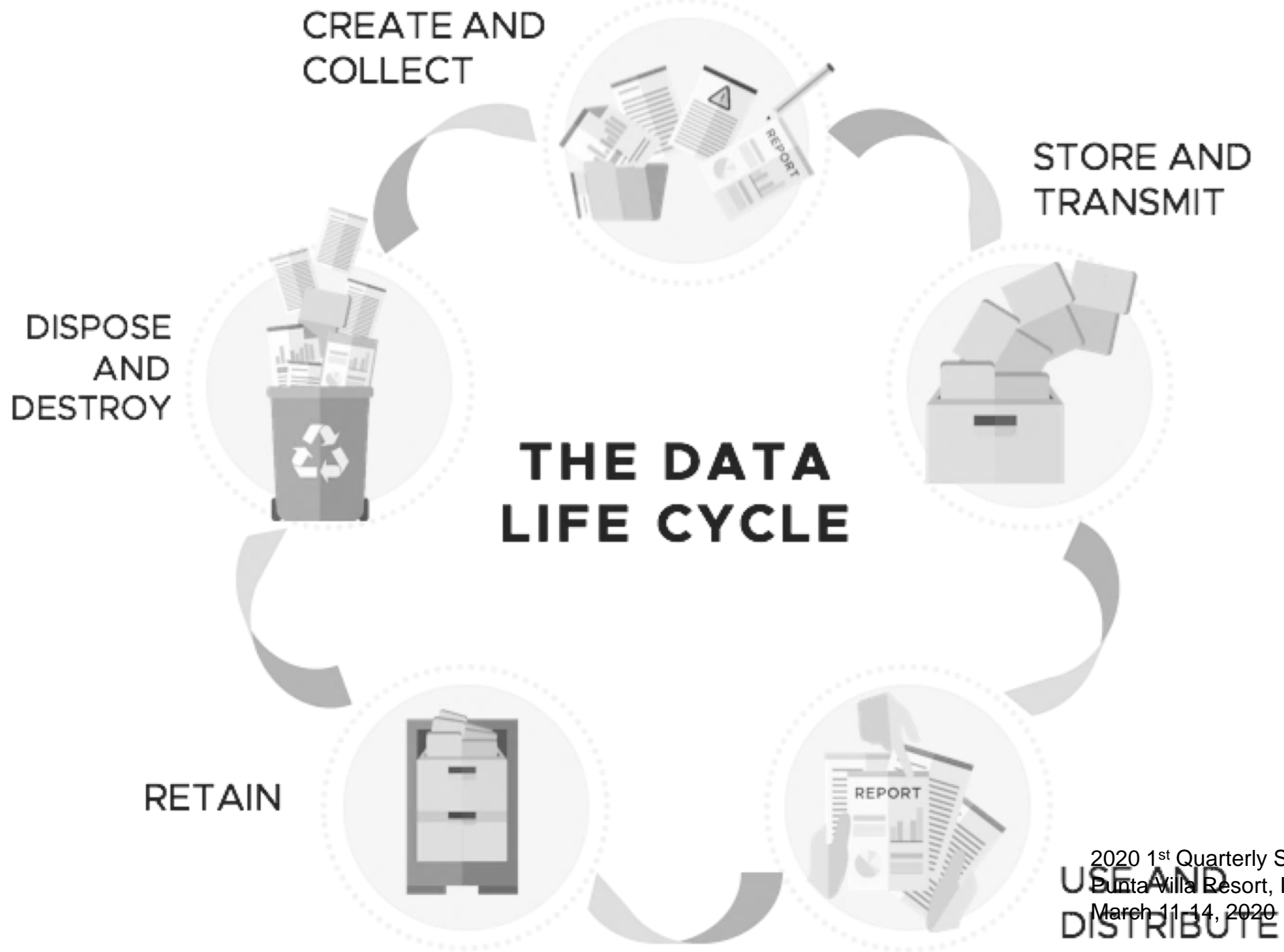


1. Race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. Health, education, genetic or sexual life of a person
3. Civil, criminal or administrative proceedings
4. Unique identifiers issued by the government agencies peculiar to an individual
5. Specifically established by law as classified.

PROCESSING



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.



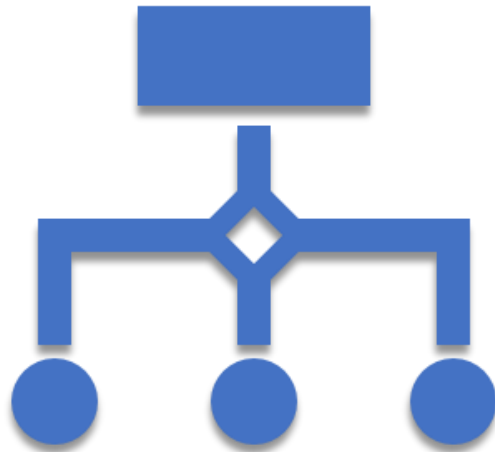
Personal Information Controller

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.

It excludes:

- ▶ A natural person who processes personal data in connection with his or her **personal, family, or household affairs**

Personal Information Processor



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.

Obligations of PICs

- ▶ Collect personal information for **specified and legitimate purposes** determined and declared before, or as soon as reasonably practicable after collection
- ▶ Collect and process personal information **adequately** and not excessively.
- ▶ Process personal information **fairly and lawfully**, and in accordance with the **rights of a data subject**.

Obligations of PICs

- ▶ process **accurate, relevant** and **up to date** personal information
- ▶ retain personal information only for **as long as necessary** for the fulfillment of the purposes for which the data was obtained.
- ▶ implement **reasonable and appropriate organizational, physical and technical measures** intended for the protection of personal information

Data Subject



An **individual** whose personal, sensitive personal or privileged **information** is **processed**.

DPA 2012
VS
EO 2 (FOI)

NPC ADVISORY NO. 2017-02

▶ **Both** intended to **benefit the public interest**, but more often than not, their provisions **complement and reinforce** each other, and are not contradictory.

The Data Privacy Act will not apply to personal information included in the FOI request which pertains to the following:



1. Information about an individual who is or was performing service under contract for a government institution that relates to the **services performed**, including the **terms of the contract**, and the **name of the individual** given in the course of the performance of those services.



2. Information relating to any discretionary benefit of a financial nature such as the **granting of a license or permit** given by the government to an individual, including the **name of the individual** and the **exact nature of the benefit**.

SECTION 5. IRR

The Act and these Rules shall not apply to Information about any individual who is or was an officer or employee of government that relates to his or her position or functions, including:

- (a) The **fact** that the individual is or was an **officer** or **employee** of the government;
- (b) The **title**, **office address**, and **office telephone number** of the individual;
- (c) The **classification**, **salary range**, and **responsibilities of the position held** by the individual; and
- (d) The **name** of the individual on a **document he or she prepared in the course of his or her employment** with the government.

SECTION 7. FOI

Protection of Privacy. While providing access to information, public records, and official records, responsible officials shall afford full protection to the right to privacy of the individual as follows:

Disclosed or released only if it is **material or relevant** to the **subject-matter** of the **request** and its **disclosure** is **permissible**;

Protect personal information in its custody or control by making **reasonable security arrangements** against leaks or premature disclosure; and

Must not disclose information except when **authorized under this order** or pursuant to existing **laws, rules or regulation**.



DATA PRIVACY PRINCIPLES

2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020



TRANSPARENCY



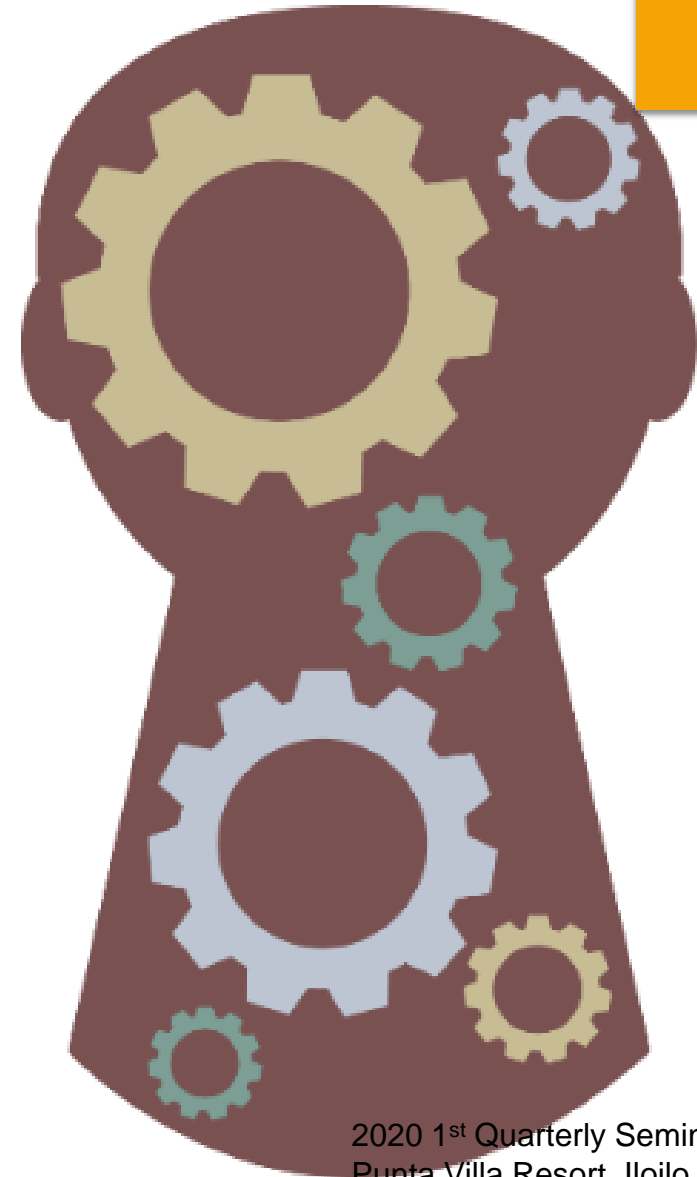
LEGITIMATE PURPOSE



PROPORTIONALITY

TRANSPARENCY

- ▶ A data subject must be aware of the **nature, purpose, and extent** of the processing of his or her personal data, including the **risks and safeguards** involved, the **identity** of personal information controller, his or her **rights** as a data subject, and how these can be **exercised**.
- ▶ Any information and communication relating to the processing of personal data should be **easy to access** and **understand**, using **clear and plain language**.



Rights of a Data Subject



1. Right to be Informed
2. Right to Access
3. Right to Object
4. Right to Rectification
5. Right to Erasure or Blocking
6. Right to Damages
7. Right to Data Portability
8. Right to File A Complaint



The right to Information

What information must be supplied?

1. **Description** of the personal data
2. **Purposes** for processing; including: direct marketing, profiling, or historical, statistical or scientific purpose
3. **Basis** of processing (legal mandate, contract, etc.)
4. **Scope and method** of the processing
5. **Recipients/classes of recipients** to whom the personal data are or may be disclosed
6. **Identity and contact details** of the personal information controller
7. **Retention** period
8. Existence of **rights** as data subjects.



The right to Information

When should information be provided?



- **before the entry** of personal data into the processing system; or
- at the **next practical opportunity**



The right to Information





The right to object

If a **data subject objects/ withholds consent**, the **PIC shall no longer process** the personal data, unless the processing is:

1. Pursuant to a **subpoena**;
2. For **obvious purposes**, i.e. contract, employer-employee relationship, etc.; or
3. Result of a **legal obligation**.



The right to access

Reasonable access to the following:

- **Contents** of personal data;
- **Sources** of personal data;
- Names and addresses of **recipients** of personal data;
- **Manner** by which such data was **processed**;
- **Reasons for the disclosure** of personal data;
- Information on **automated processes**;
- Date when personal data was **last accessed/modified**; and
- **Name/ address** of the PIC.



The right to erasure or blocking

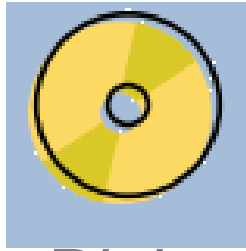
When does the right apply?

- a. When personal data is:
 - **incomplete, outdated, false, or unlawfully obtained**
 - used for **unauthorized purpose**
 - **no longer necessary** for the purpose
- b. Data subject **withdraws consent/objects** to the processing, and there is **no other legal ground/legitimate interest** for processing
- c. Processing is **unlawful**
- d. PIC or PIP **violated the rights** of the data subject



The right to rectification

- **Dispute the inaccuracy or error** in the personal data and have the PIC **correct it immediately**.
- If personal data was **disclosed to third parties: PIC must inform** them of the **rectification** upon reasonable request of the data subject.



The right to data portability

Right to **obtain** from the PIC a **copy of personal data** in an **electronic/ structured format**.

What are the **conditions** for this right to apply?

- ✓ personal data requested **concerns the data subject** making the request;
- ✓ personal data is **processed electronically**;
- and
- ✓ processing is **based on consent or contract**.



The right to damages

The data subject shall be **indemnified for any damages** sustained due to such **inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data**, taking into account any violation of his or her **rights and freedoms** as data subject.

LEGITIMATE PURPOSE

- ▶ The processing of information shall be compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy.



Consent

- ▶ The data subject agrees to the collection and processing
 - ▶ Freely given
 - ▶ Specific
 - ▶ Informed indication of will
- ▶ Evidenced by written, electronic or recorded means:
 - ▶ signature
 - ▶ opt-in box/clicking an icon
 - ▶ sending a confirmation email
 - ▶ oral confirmation

Consent

- Consent means giving data subjects **genuine choice and control** over how a PIC uses their data.
- Consent should be **unbundled from other terms and conditions** (including giving granular consent options for different types of processing) wherever possible.
- Clear affirmative action means someone must take **deliberate action to opt in**.

Is consent always needed?

- ▶ **No.** Consent is just **one criterion** for lawful processing of both personal and sensitive personal information.
- ▶ Consent will **not always be the most appropriate basis** for processing personal data.
- ▶ PICs should **choose the lawful basis that most closely reflects the true nature of the relationship** with the individual and the purpose of the processing.

Processing which may not need consent:



Contract: to supply goods or services they have requested, or to fulfil your obligations under an employment contract. This also includes steps taken at their request before entering into a contract.

Compliance with a legal obligation: if you are required by law to process the data.

Vital interests: you can process personal information if it is necessary to protect the data subject's life and health.

National emergency: to respond to national emergency or to comply with the requirements of public order and safety.

Public task: if you need to process personal information to carry out public function or service and you have a legal basis for the processing.

Legitimate interests: for the private sector, you can process personal data without consent if you have a genuine and legitimate reason, unless this is overridden by fundamental rights and freedoms of the data subject.

What are the alternatives to consent?

For processing of **personal information:**

What are the alternatives to consent?

For processing of sensitive personal information:



Existing law and regulation: you can process sensitive personal information (SPI) when there is a regulatory enactment which requires the processing



Protection of life and health: to protect someone's life – the data subject or another person, and the data subject is not legally/physically able to express his consent



Public organizations: refers to processing done by non-stock, non-profit organizations, cooperatives, and the like, where processing is only confined and related to the bona fide members



Medical treatment: when processing is carried out by a by a medical practitioner or a medical treatment institution, and there is adequate level of protection



Lawful rights and interests: when processing is necessary to protect lawful rights and interests of in court proceedings, in the establishment/ exercise/defense of legal claims or when provided to government or public authority

PROPORTIONALITY

► The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.



PARA MAKAUTANG..

(PLEASE BRING THIS REQUIREMENTS)

- 6pcs 2x2 PICTURE
- 4pcs 1x1 PICTURE (WHOLE BODY)
- 3 VALID ID'S
- BRGY. CLEARANCE
- NBI CLEARANCE
- MAYORS PERMIT
- MEDICAL
- CEDULA
- BIRTH CERTIFICATE (NSO)
- SSS/TIN
- CO-MAKER
- X-RAY (WHOLE BODY)
- POLICE CLEARANCE
- PROOF OF BILLING
- FORM 137



San Juan

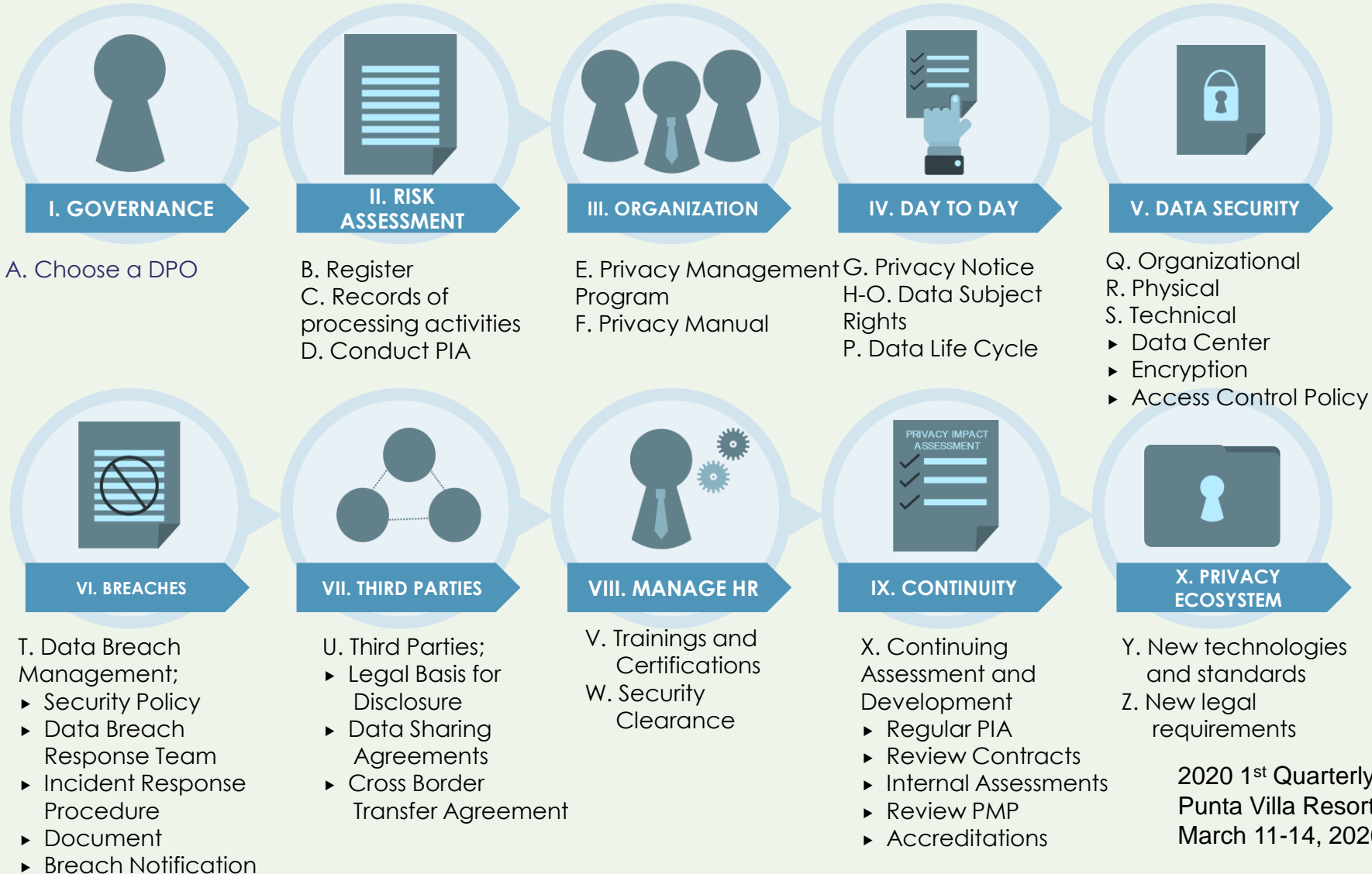
Like This Page - February 8 - Edited -

020 Seminar & Meeting
Punta Villa Resor
to City
March 11-14, 202

The NPC's 5 Pillars of Accountability and Compliance



THE NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK



2020 1st Quarterly Seminar & Meeting
 Punta Villa Resort, Iloilo City
 March 11-14, 2020

A cartoon illustration of a man with dark hair and glasses, wearing a suit and tie. He is holding a large white sign with the letters 'DPO?' written in a bold, orange font. The background is a dark blue gradient with a pattern of small white dots. In the top right corner, there is a solid orange rectangular shape.

I. GOVERNANCE

A. CHOOSE A DATA PROTECTION OFFICER (DPO)

2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020

II. RISK ASSESSMENT

- ▶ B. Register
- ▶ C. Records of processing activities
- ▶ D. Conduct PIA (Privacy Impact Assessment)

B. Register (NPC Circular 17-01)

- ▶ What to register?
 - ▶ Registration of your Data Protection Officer
- ▶ Who should register?
 - ▶ the PIC or PIP employs at least two hundred fifty (250) employees;
 - ▶ the processing includes sensitive personal information of at least one thousand (1,000) individuals; and
 - ▶ the processing is likely to pose a risk to the rights and freedoms of data subjects.

Registration of PICs and PIPs

Validity of Registration

Extended until **AUGUST 31, 2020**

Renewal of Registration

Begins on **JULY 1, 2020**

For those who have yet to register

Please visit **privacy.gov.ph**
for instructions

D. Conduct PIA (Privacy Impact Assessment)





Republic of the Philippines
NATIONAL PRIVACY COMMISSION
RECORDS OF PROCESSING ACTIVITIES

(NOTE: This guide is used for each processing activity.

The data in this guide will be use in the conduct of your Privacy Impact Assessment.)



Name of Organization:			
Email:		Contact Number:	
Data Protection Officer:			
Contact Details:	Email:		
	Contact Number:		

NO.	NAME <i>(State the name of the data processing system.)</i>	DATA SUBJECTS <i>(Check and specify the data subjects.)</i>
		<input type="checkbox"/> Employees <input type="checkbox"/> Clients <input type="checkbox"/> Students <input type="checkbox"/> Patients <input type="checkbox"/> Staffs <input type="checkbox"/> Consultants Others: <i>(Please state)</i>

PURPOSE OF PROCESSING <i>(State the information about the purpose of the processing of personal data, including any intended future processing or data sharing.)</i>	
2020 1 st Quarterly Seminar & Meeting Punta Villa Resort, Iloilo City March 11-14, 2020	

TYPE OF SYSTEM			MANAGING AS			SUBCONTRACTED	
<input type="checkbox"/> Manual	<input type="checkbox"/> Electronic	<input type="checkbox"/> Both	<input type="checkbox"/> Personal Information Controller (PIC)	<input type="checkbox"/> Personal Information Processor (PIP)	<input type="checkbox"/> Both	<input type="checkbox"/> Yes	<input type="checkbox"/> No
GENERAL INFORMATION							
<i>(State the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data. List all personal data (e.g. Personal Full Name, address, gender, phone number, etc.) and state which is/are the sensitive personal information (e.g. race, ethnicity, marital status, health, genetic, government issued numbers).)</i>							
DESCRIPTION OF SECURITY MEASURES							
<i>(State a general description of the security measures in place.)</i>							
TO WHOM THE PERSONAL DATA IS BEING DISCLOSED THROUGH THIS PROCESSING ACTIVITY?							
<i>(State to whom the personal data is being disclosed.)</i>							

III. ORGANIZATION

- ▶ E. Privacy Management Program
- ▶ F. Privacy Manual



2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020

IV. DAY TO DAY



**G. PRIVACY
NOTICE**



**H - O. DATA
SUBJECT RIGHTS**



**P. DATA LIFE
CYCLE**



Privacy Notice

- ▶ Description of the personal information to be entered into the system;
- ▶ Purposes for which they are being or are to be processed;
- ▶ Scope and method of the personal information processing;
- ▶ The recipients or classes of recipients to whom they are or may be disclosed



Privacy Notice

- ▶ Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
- ▶ The identity and contact details of the personal information controller or its representative;



Privacy Notice

- ▶ The period for which the information will be stored; and
- ▶ The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

Data Subjects' Rights

1. Empowers Data Subjects
2. Transparent
3. Compelling



The right to information



The right to access



The right to rectification



The right to data portability



The right to object



The right to erasure or blocking



The right to file a complaint



The right to damages



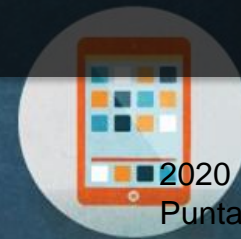
Privacy Notice

Data Subjects' Rights

IV. DATA SECURITY

- ▶ Q. Organizational
- ▶ R. Physical
- ▶ S. Technical

Data
Security



Q. Organizational

► Involves implementing policies and programs explicitly intended to ingrain the culture of privacy into an organization's psyche, thus making it impervious to hackers who resort to social engineering ploys.



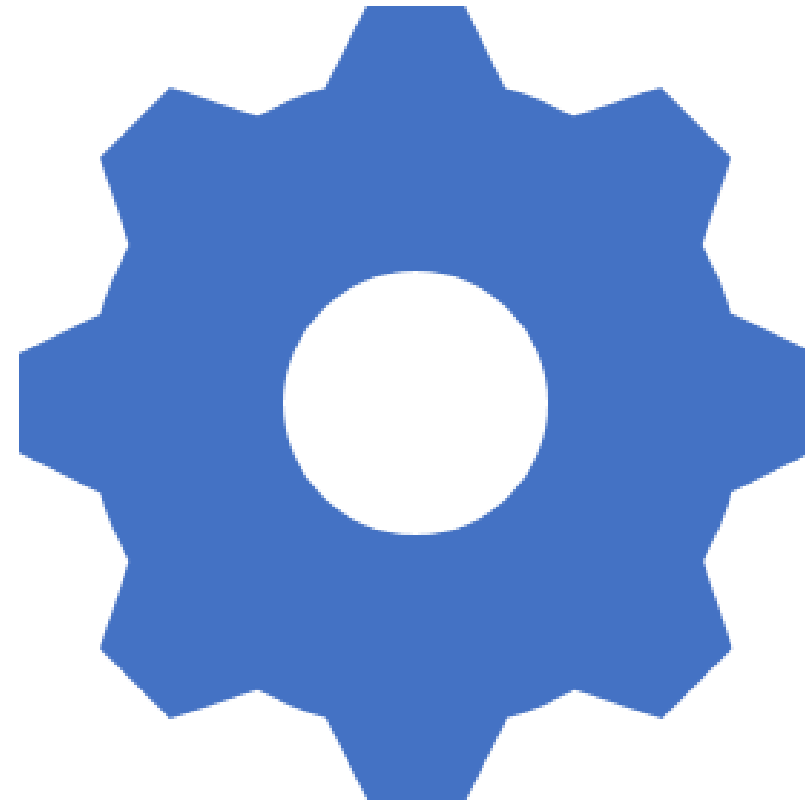
R. Physical

► Refers to the practical protective schemes such as provision for security guards, padlocks, lockers and secluded archives to physically protect paper records and databases against data thieves who may resort to brute force.



S. Technical

► Covers all proactive and defensive IT solutions an organization could employ in securing its data assets against all types of breaches. This may include the use of robust firewall and encryption systems, rigorous data access protocols, as well as anti-virus and anti-spyware solutions.



VI. BREACHES

T. Data Breach Management

- ▶ Security Policy
- ▶ Data Breach Response Team
- ▶ Incident Response Procedure
- ▶ Document
- ▶ Breach Notification



2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020

Security Incident



- ▶ An event or occurrence that affects or tends to affect data protection; or
- ▶ May compromise the availability, integrity, and confidentiality of personal data.
- ▶ Includes incidents that may result in a personal data breach, if not for safeguards that have been put in place.

Personal Data Breach

- ▶ Availability breach
 - ▶ loss, accidental or unlawful destruction of personal data;
- ▶ Integrity breach
 - ▶ alteration of personal data
- ▶ Confidentiality breach
 - ▶ unauthorized disclosure of or access to personal data.



A **personal data breach** is a breach of security resulting to accidental or unlawful destruction, loss, or alteration of personal data, including its unauthorized disclosure.



PRIVACY BREACHES: **Examples**



lost or stolen laptops, removable storage devices, or paper records containing personal information

hard disk drives and other digital storage media being disposed of or returned to equipment lessors without the contents first being erased

databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the agency or organization

employees accessing or disclosing personal information outside the requirements or authorization of their employment

Must have **at least one member** with the **authority to make immediate decisions on critical actions.**

The team shall be **responsible** for:

- **Implementation** of the security incident management policy
- **Management** of security incidents and personal data breaches
- **Compliance** with the data privacy law and other issuances

DATA BREACH RESPONSE TEAM

REQUISITES

Notification of a data breach is **mandatory** when:



It involves sensitive personal information that may be used for identity fraud.

All three elements must be present!



likely to give rise to a significant risk of serious harm to the affected subjects.

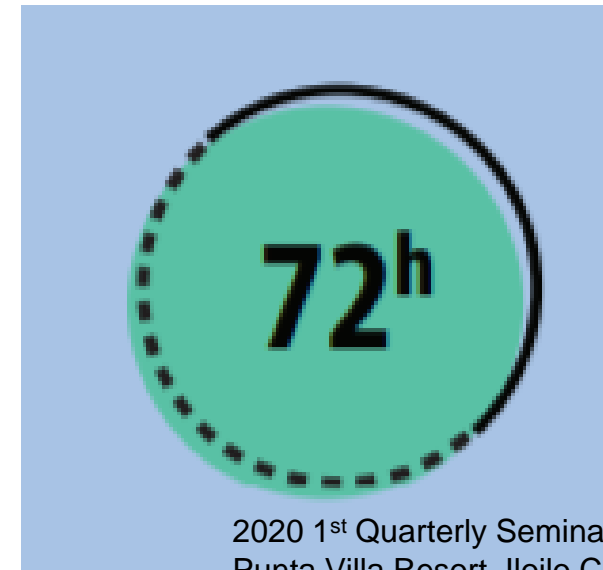
WHO SHOULD BE NOTIFIED?



Notification must be made to the **Commission** and to any **affected data subjects**.

WHEN TO NOTIFY

- ▶ The notification must be made **within 72 hours** upon knowledge of, or when there is reasonable belief that a personal data breach has occurred.



2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020

ANNUAL REPORT

- ▶ **All security incidents and personal data breaches** shall be documented through written reports, **including** those **not covered by the notification requirements**. Any or all reports shall be made available when requested by the Commission.
- ▶ **Aggregated data** for security incidents not involving a personal data breach suffices.

SUMMARY REPORT

▶ A **summary of all reports** comprised of general information submitted to the Commission annually.



VII. THIRD PARTIES

- ▶ U. Third Party Relationship
 - ▶ Legal Basis for Disclosure
 - ▶ Data Sharing Agreements
 - ▶ Cross Border Transfer Agreement

OUTSOURCING AGREEMENT



shall set out the **subject-matter** and **duration** of the processing,



the **nature and purpose** of the processing,



the **type of personal data** and **categories of data subjects**,



the **obligations and rights** of the **personal information controller**, and



the **geographic location** of the **processing** under the subcontracting agreement.

2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020

Data Sharing Agreement



consent of data subjects



establishment of **adequate safeguards** for data privacy and security, and **upholding of the rights** of data subjects



provide data subjects with the required information prior to collection or before data is shared, and



adherence to the data privacy principles.

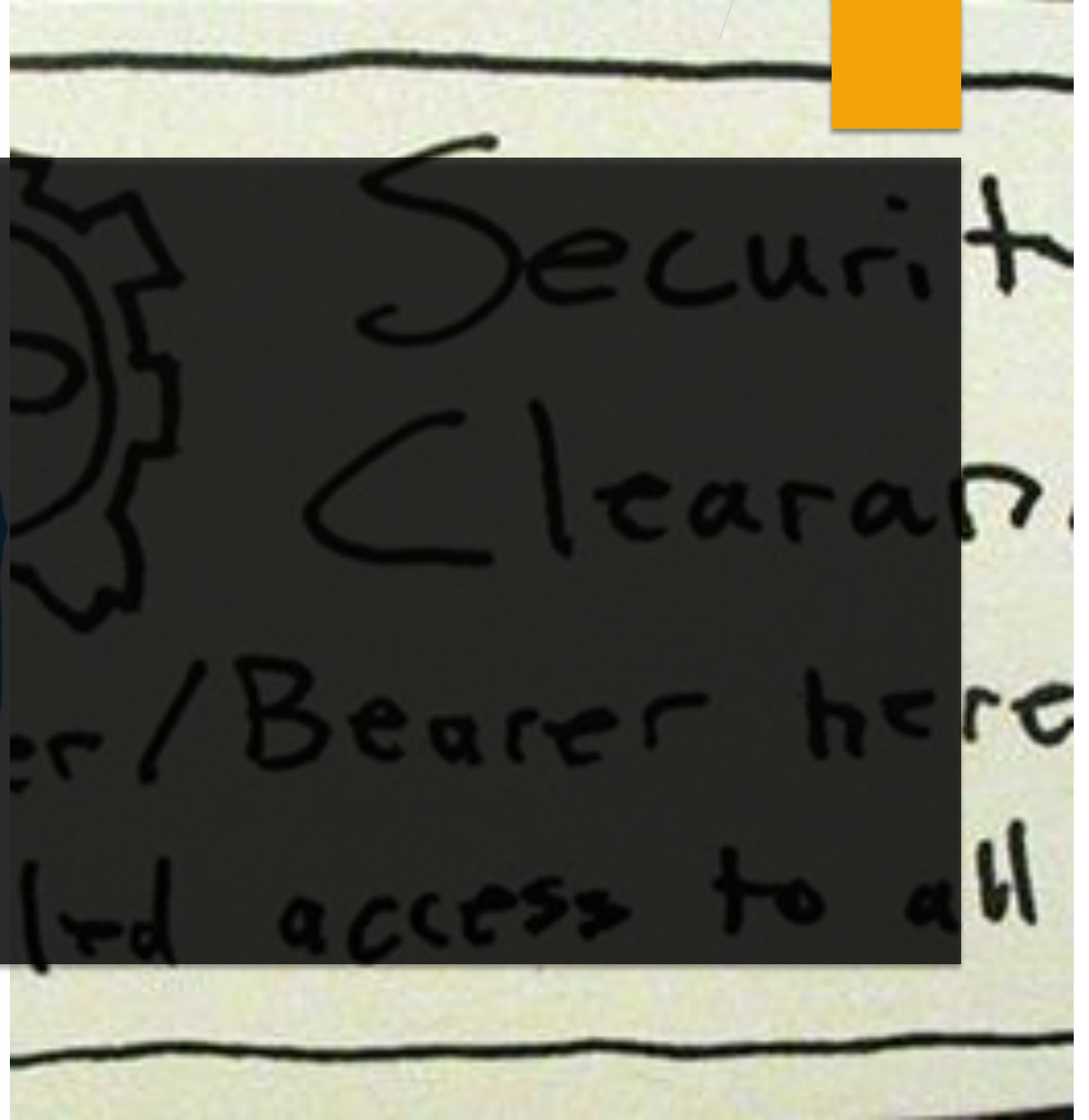
CROSS BORDER TRANSFER AGREEMENT

- ▶ A personal information controller shall be responsible for any personal data under its control or custody, **including** information that have been **outsourced or transferred to a personal information processor** or a third party for processing, whether **domestically or internationally**, subject to cross-border arrangement and cooperation.

CERTIFICATION

VIII. MANAGE HR

- ▶ V. Trainings and Certifications
- ▶ W. Security Clearance



Training and Capacity Building

- ▶ PIC/PIP must provide for **Capacity building, orientation or training programs** regarding privacy and security policies for employees, agents or representatives, particularly those who will have **access to personal data**.

Security Clearance and Non-Disclosure Agreement

- ▶ **Security Clearance** – allows authorized access to Personal Information that would **otherwise be forbidden**. Only **grant access** to an employee when the performance of his/her **function directly depends on and cannot otherwise be performed unless access** to personal data is **allowed**.
- ▶ **Non-Disclosure Agreement** – legal contract that outlines the **confidential materials, knowledge, or information** that the **parties will share** with one another. Set out what information are confidential and those that are not.

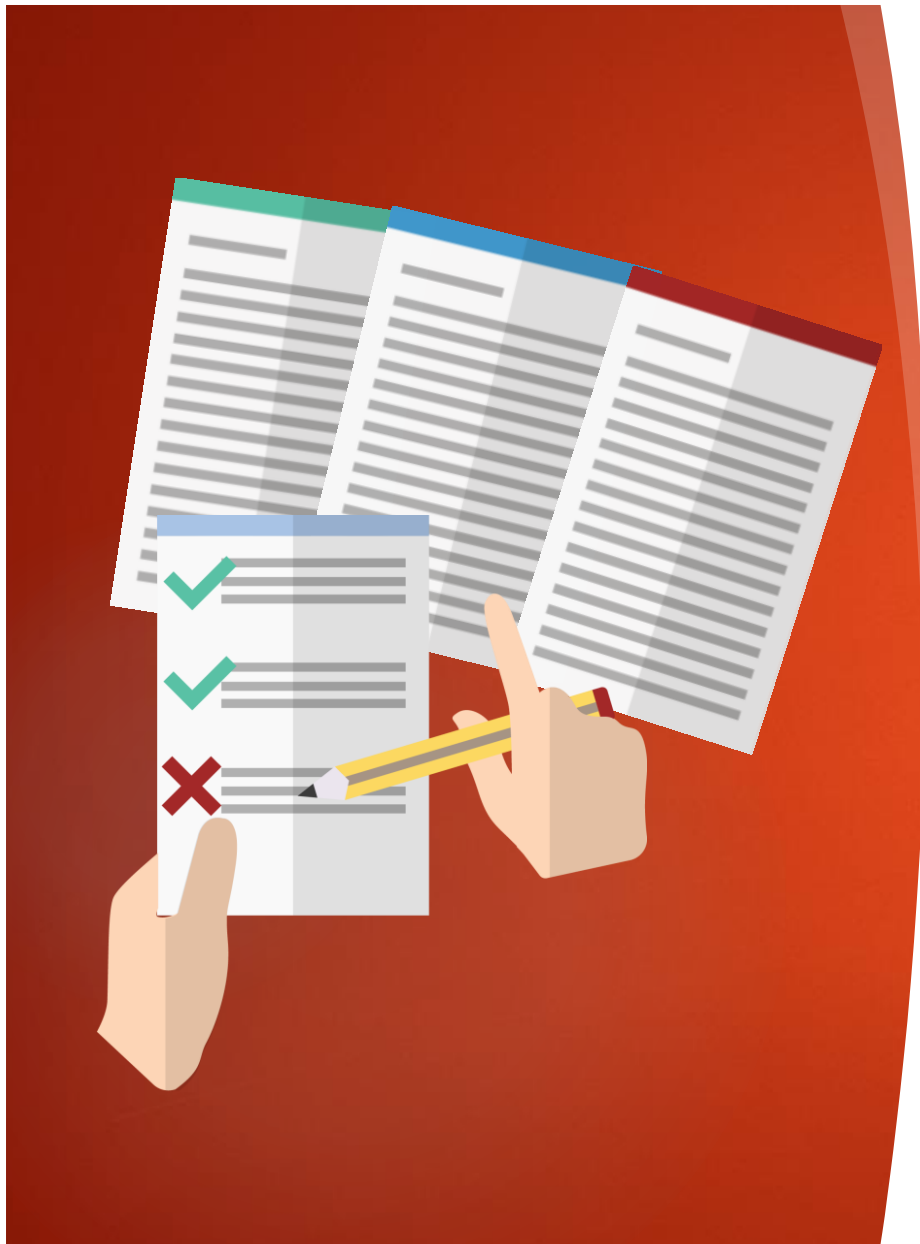


- ▶ X. Continuing Assessment and Development
 - ▶ Regular PIA (Private Impact Assessment)
 - ▶ Review Contracts
 - ▶ Internal Assessments
 - ▶ Review and update PMP and Privacy Manual
 - ▶ Accreditations

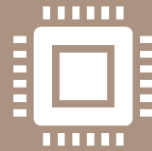
IX. CONTINUITY

- ▶ Y. New technologies and standards
- ▶ Z. New legal requirements

X. PRIVACY ECOSYSTEM



The legal counsel or legal department must **keep itself abreast of any or all policy developments involving data privacy**, particularly those issued by the NPC. It has the duty to inform the organization of any significant updates, through the issuance of appropriate memoranda or advisories.



The IT Team must **monitor emerging technologies, new risks in data processing and the privacy ecosystem**



Both must **keep track of data privacy best practices**, sector specific standards, international data protection standards.



2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020

Punishable Acts

- ▶ **Unauthorized Processing** of Personal Information and Sensitive Personal Information
- ▶ **Accessing** Personal Information and Sensitive Personal Information **Due to Negligence**
- ▶ **Improper Disposal** of Personal Information and Sensitive Personal Information
- ▶ **Processing** of Personal Information and Sensitive Personal Information for **Unauthorized Purposes**
- ▶ **Unauthorized Access or Intentional Breach**
- ▶ Concealment of Security Breaches Involving Sensitive Personal Information
- ▶ **Unauthorized Disclosure**

Punishable Acts

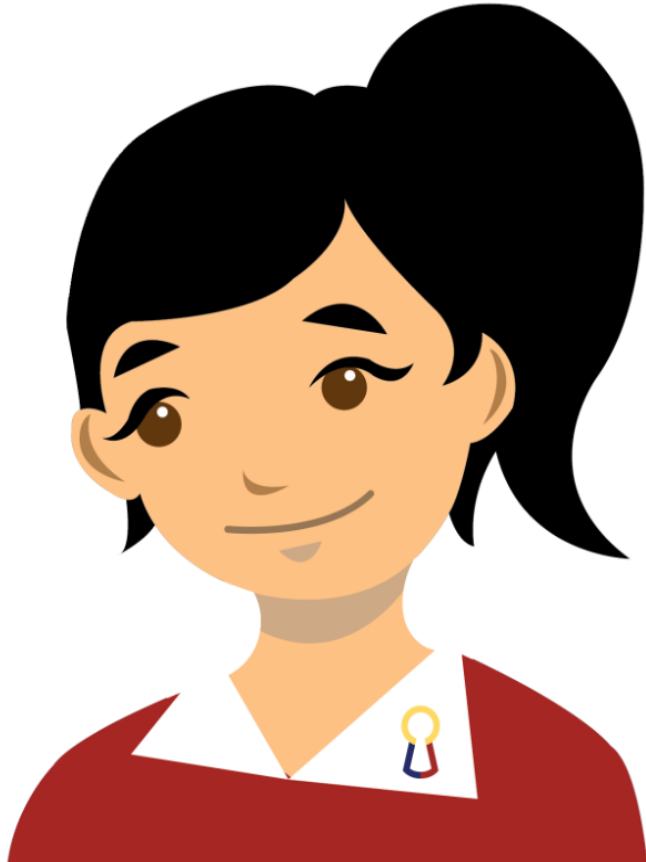
- ▶ Combination or Series of Acts
- ▶ Large-Scale
 - ▶ the personal information of **at least one hundred (100)** persons is harmed, affected or involved as the result of the above mentioned actions



If you can't
protect it,
don't collect it

THE DATA PRIVACY GOLDEN RULE

8234-2228



Complaints : Loc 114

Compliance/
Registration : Loc 118

Public assistance : Loc 116/117

Email us at info@privacy.gov.ph

AskPriva

Thank you!



2020 1st Quarterly Seminar & Meeting
Punta Villa Resort, Iloilo City
March 11-14, 2020