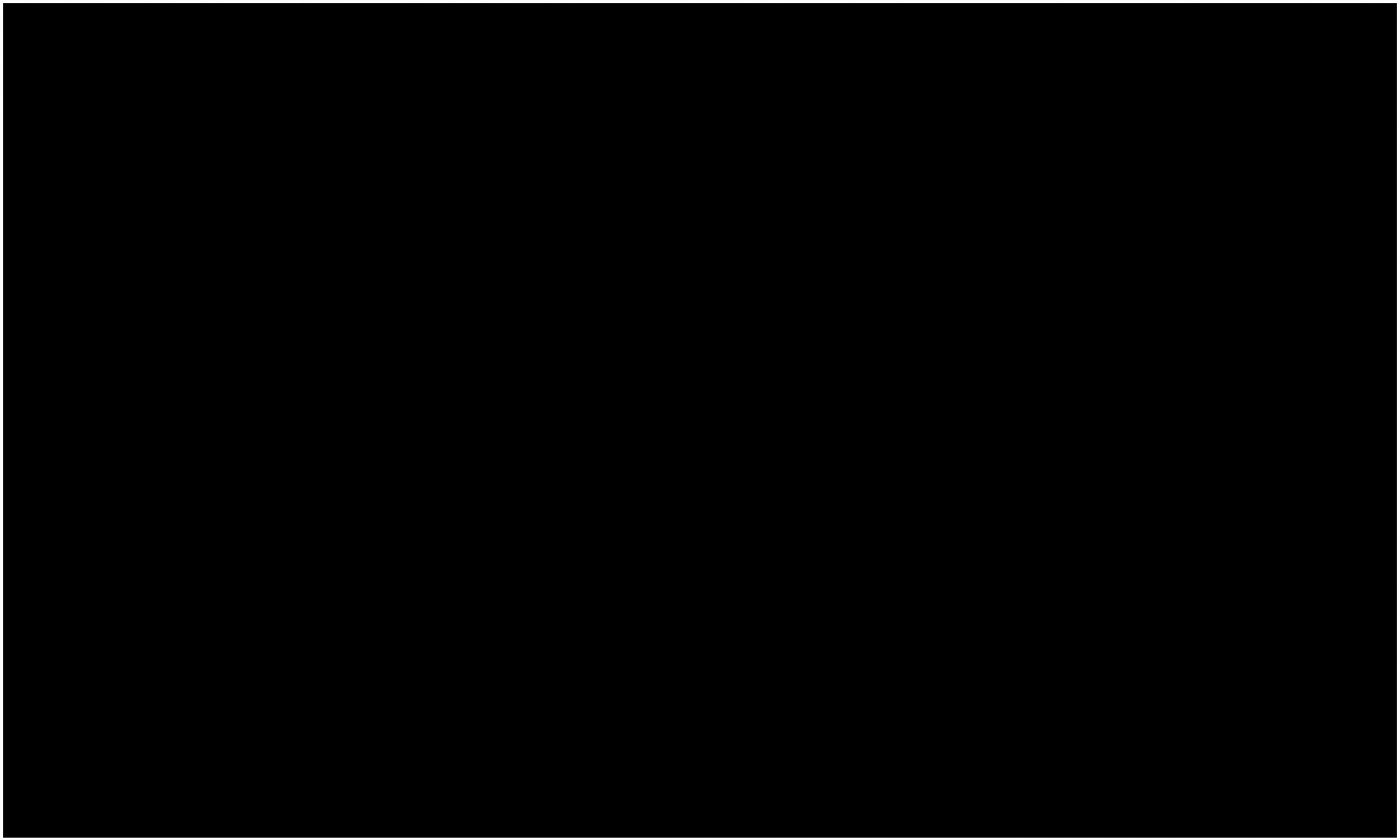
Managing Data Privacy Risks and Maintaining Regulatory Compliance

Atty. Anna Benjieline R. Puzon, J.D., CIPP/E, CC
Attorney IV, Compliance and Monitoring Division



4400%

Production of data is expanding at an exponential rate

Companies like….

FACEBOOK **GOOGLE** **APPLE**

Have been harnessing data from their users and monetizing it.. sometimes without the users even knowing it

DATA

10101010101010101010101010101010101010101010101010101
01010101010101010101010101010101010101010101010101010
10101010101010101010101010101010101010101010101010101
01010101010101010101010101010101010101010101010101010
10101010101010101010101010101010101010101010101010101
01010

We are in a digital economy where data is more valuable than ever. It's the key to the smooth functionality of everything from the government to local companies. Without it, progress would halt.

DATA-DRIVEN INCIDENTS

- The secret and sensitive data of literally hundreds of millions of people has been exposed and aggregated on various dark webs lists for sale!
- Data breaches are a terrifying top trend in the digital world. What's more, they're showing no sign of slowing down any time soon.

14,717,618,286

Data breaches have been lost or stolen since **2013**.

6,500,715 records

Data records compromised everyday

4%

Only 4% of breaches where secured breaches, where encryption was used and the stolen data was rendered useless.

75

Records compromised every minute

BAGONG PILIPINAS

NATIONAL PRIVACY COMMISSION

ISO 9001:2015 CERTIFIED

PERSONAL DATA BREACH NOTIFICATIONS FY 2022

REPORTED PERSONAL DATA BREACH THROUGH DATA BREACH NOTIFICATION MANAGEMENT SYSTEM ('DBNMS') FY 2022	
Government	29
Private	178
Total Personal Data Breach (without invalid notification)	**208**

TOP 5 Sectors reporting Data Breach Notifications	
Financial Service Activities	39
Others	19
Education	18
Healthcare Facilities	17
Office Administrative, Office Support and other Business Support; Retail/Trade	12 12

GENERAL CAUSES	
System Glitch/Human Error	8
Malicious Attack	79
Human Error	81
System Glitch	14
Malicious Attack/Human Error	24
Malicious Attack/System Glitch	2
TOTAL	***208***

SPECIFIC CAUSES	
Hacking Incident	38
Theft	11
Lost/misdelivery of document	30
Personnel Error	41
Phishing	5
Stolen gadget/laptop	2
System error/vulnerability	32
Unauthorized Access	0
Unauthorized disclosure	7
Others	42
TOTAL	***208***

PERSONAL DATA BREACH NOTIFICATIONS FY 2023

REPORTED PERSONAL DATA BREACH THROUGH DATA BREACH NOTIFICATION MANAGEMENT SYSTEM ('DBNMS') FY 2023	
Government	52
Private	231
Total Personal Data Breach (without invalid notification)	**283**
Total Personal Data Breach (with invalid notification)	**303**

TOP 5 Sectors reporting Data Breach Notifications	
Government	52
Bank/Financing Leasing	38
Others	36
Retail	23
Health	17

GENERAL CAUSES	
System Glitch/Human Error	9
Malicious Attack	130
Human Error	115
System Glitch	10
Malicious Attack/Human Error	15
Malicious Attack/System Glitch	4
TOTAL	***283***

SPECIFIC CAUSES	
Hacking Incident	51
Theft	13
Lost/misdelivery of document	30
Personnel Error	83
Phishing	7
Stolen gadget/laptop	2
System error/vulnerability	13
Unauthorized Access	0
Unauthorized disclosure	1
Others	83
TOTAL	***283***

PERSONAL DATA BREACH NOTIFICATIONS FY 2024

(January 01-July 31, 2024)

REPORTED PERSONAL DATA BREACH THROUGH DATA BREACH NOTIFICATION MANAGEMENT SYSTEM ('DBNMS') FY 2024 (January 01- July 31, 2024)	
Government	51
Private	163
Total Personal Data Breach (without invalid notification)	**214**
Total Personal Data Breach (with invalid notification)	**230**

TOP 5 Sectors reporting Data Breach Notifications (January 01- July 31, 2024)	
Government	51
Education	19
Financial Service Activities	19
Manpower Agencies	15
Others	10

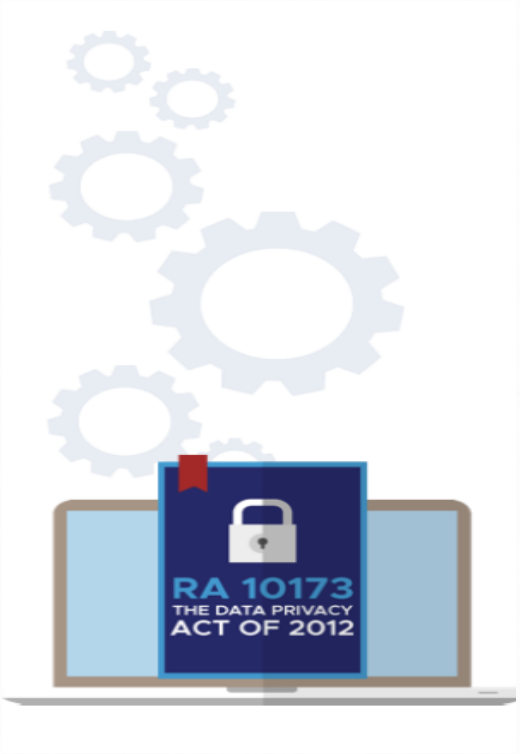
GENERAL CAUSES	
System Glitch/Human Error	4
Malicious Attack	96
Human Error	70
System Glitch	6
Malicious Attack/Human Error	33
Malicious Attack/System Glitch	5

SPECIFIC CAUSES	
Hacking Incident *(Hacking Cloud, Hacking-Database, Hacking-Email Account, Hacking-Infrastructure, Hacking-Server, Hacking-Website, Hacking-Others, Hacking-SQL Injection, Hacking-Phishing, Hacking-Man-In-The Middle)*	62
Theft	1
Lost/misdelivery of document *(Loss of Document, Misdelivered Document, Loss of Equipment)*	26
Personnel Error *(Accidental Email, Negligence, Misuse of Resources, Undertrained staff)*	25
Phishing	2
Stolen gadget/laptop *(Stolen device)*	1
System error/vulnerability *(Connection ERror, Hardware Failure, System Error, System Configuration, Malware Ransomware, Malware-Trojan Horse, Insider Threat, Malware-Virus)*	25
Unauthorized disclosure	7
Others	65
TOTAL	214

INTRODUCTION: RA 10173

DATA PRIVACY ACT OF 2012

An act **protecting individual personal information** in information and communications systems in the government and the private sector, creating for this purpose a **National Privacy Commission**, and for other purposes.



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.

How do we maintain regulatory compliance?

Let's define key concepts first.

SCOPE

SEC. 4. Applies to the processing of all types of personal information, in the country and even abroad, subject to certain qualifications.

SCOP

Does not apply to the following:

(a) Information about any individual who is or was an **officer or employee of a government institution** that relates to the position or functions of the individual

(b) Information about **an individual who is or was performing service under contract for a government institution** that relates to the services performed

(c) 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

(d) Personal information processed for **journalistic, artistic, literary or research purposes**

NATIONAL PRIVACY COMMISSION

SCOP

(e) Information necessary in order to carry out the **functions of public authority**

(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas **to comply with Republic Act No. 9510 (CISA Law), and Republic Act No. 9160 (AMLA)** and other applicable laws

(g) Personal information originally collected from **residents of foreign jurisdictions**

Note: *only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned*

NATIONAL PRIVACY COMMISSION

CLASSIFICATION OF PERSONAL DATA

PERSONAL INFORMATION (PI)

- 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**.
- Processing is **generally allowed** in accordance to **Sec. 12**

SENSITIVE PERSONAL INFORMATION (SPI)

- Race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- 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 person, the disposal of such proceedings, or the sentence of any court in such proceedings;
- Issued by government agencies peculiar to an individual (social security numbers, health records, licenses or its denials, suspension or revocation, and tax returns); and
- Specifically established by law to be kept classified.
- Processing is **prohibited** except as provided in **Sec. 13**

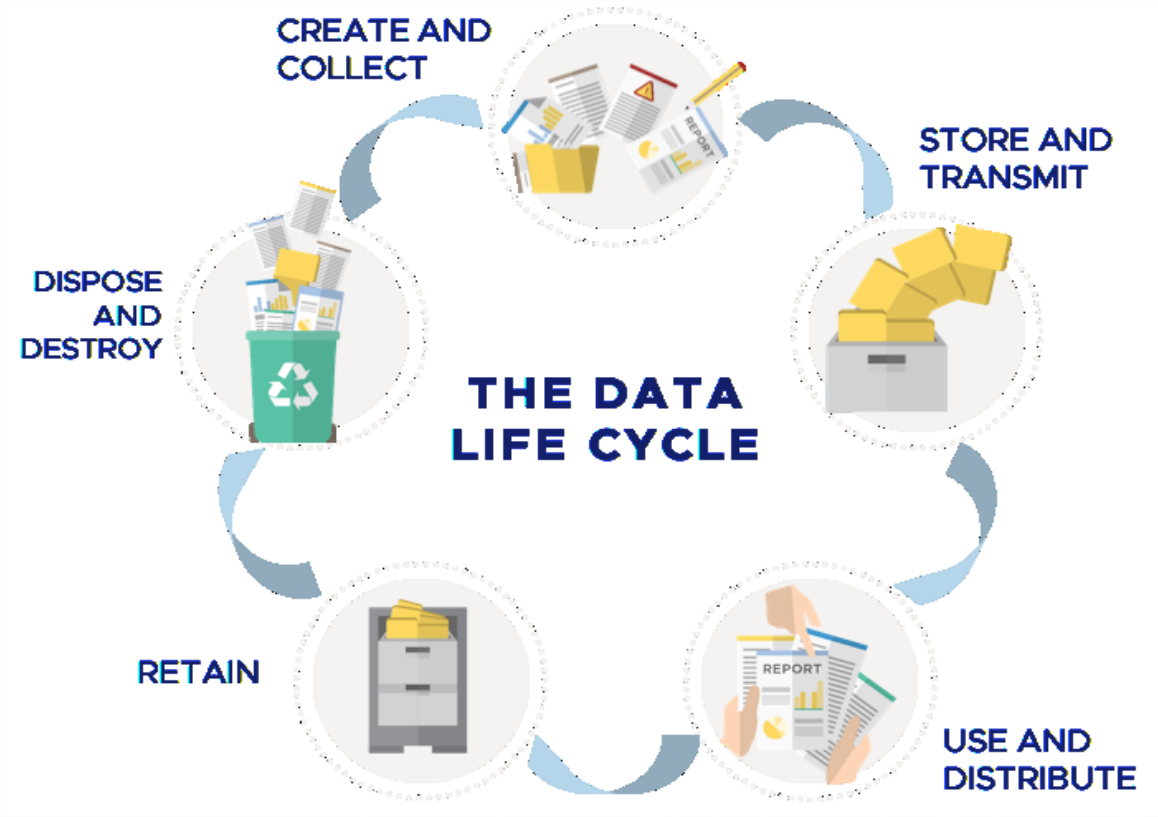
PRIVILEGED INFORMATION

- Husband-Wife
- Lawyer- Client
- Doctor-Patient
- Priest-Penitent
- any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication

PROCESSING

Any operation of **any set of operations performed upon personal data** including, but not limited to the following:

- ✓ Collection
- ✓ Recording
- ✓ Organization
- ✓ Storage
- ✓ Updating or modification
- ✓ Retrieval
- ✓ Use
- ✓ Consolidation
- ✓ Blocking
- ✓ Erasure
- ✓ Destruction
- ✓ Consultation


CREATE AND COLLECT
STORE AND TRANSMIT
USE AND DISTRIBUTE
RETAIN
DISPOSE AND DESTROY
THE DATA LIFE CYCLE
REPORT
REPORT

DATA SUBJECT

An individual whose **PERSONAL INFORMATION, SENSITIVE PERSONAL INFORMATION, or PRIVILEGED INFORMATION** is being processed

PERSONAL INFORMATION CONTROLLER (PIC)

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.

PERSONAL INFORMATION PROCESSOR (PIP)

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.

PROCESS OWNER

People within the organization who **plays a role** in ensuring compliance by the PIC or PIP with the Data Privacy Act, its IRR, related issuances of the National Privacy Commission, and other applicable laws and regulations relating to data privacy and security.

T – L – P

DATA PRIVACY PRINCIPLES

TRANSPARENCY

The data subjects must be aware of the nature, purpose, extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of PIC, 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.

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

PROPORTIONALITY

The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

Processing only if the purpose could not be reasonably fulfilled by other means.

C – I – A

INFORMATION SECURITY PRINCIPLES

CONFIDENTIALITY

Confidentiality is the protection of information from unauthorized access. Confidentiality requires measures to ensure that only authorized people are allowed to access the information.

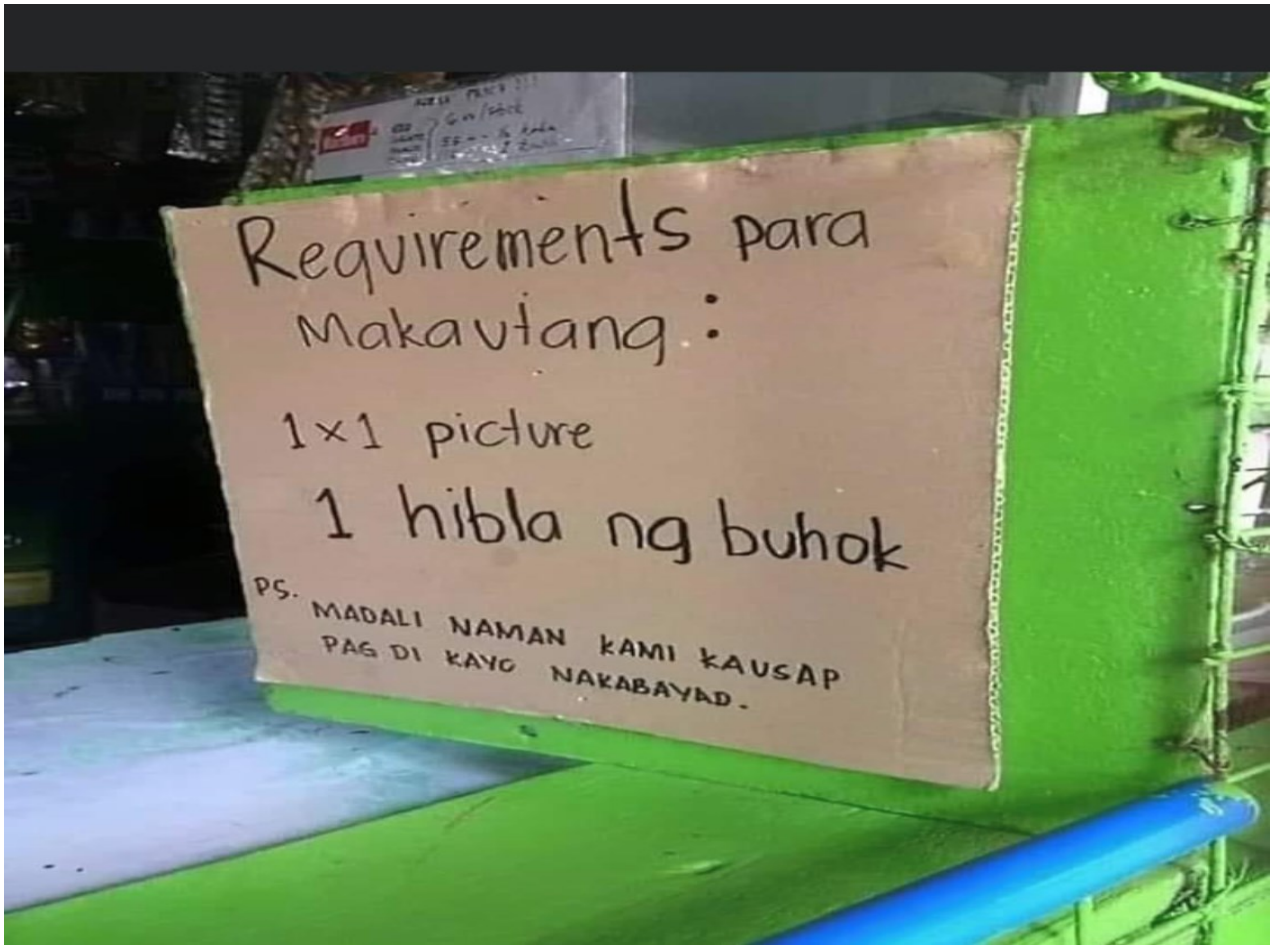
INTEGRITY

The goal of integrity is the condition where information is kept accurate and consistent unless authorized changes are made. Integrity relates to information security because accurate and consistent information is a result of proper protection.

AVAILABILITY

Availability is maintained when all components of the information system are working properly. Problems in the information system could make it impossible to access information, thereby making the information unavailable.

NATIONAL PRIVACY COMMISSION



NATIONAL
PRIVACY
COMMISSION

Criteria for Lawful Processing

Sections 12 & 13 of the DPA

Personal Information	Sensitive Personal Information
Consent	Consent
Law and Regulation	Law and Regulation
Protect Life	Protect Life
Contract	Lawful and Noncommercial Objectives of Public Organizations and their Associations
Legal Obligation	Medical Treatment
Public Order and Safety, government mandate	Court Proceedings, Legal Claims
Legitimate Interest	

Legitimate Purpose: Consent

- The data subject agrees to the collection and processing of personal information

  - ✓**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

- **Opt-in**: silence, pre-ticked boxes or inactivity does not constitute consent

NATIONAL PRIVACY COMMISSION

Legitimate Purpose: Consent

- Consent means giving data subjects genuine choice and control over how a PIC uses their data.

- Data subjects must be able to refuse consent, and must be able to withdraw consent easily at any time.

- 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

NATIONAL PRIVACY COMMISSION

Criteria for Lawful Processing of Personal Information (Sec. 12)

1. The data subject must have given **consent** prior to the collection, or as soon as practicable and reasonable;

2. Processing involves the personal information of a data subject who is a party to a **contractual agreement,** or in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to enteri agreement;

3. Processing necessary for **compli legal obligatio** which th subject;

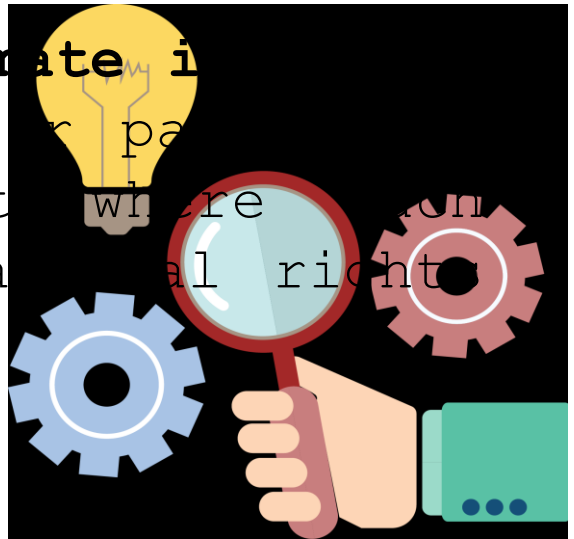
NATIONAL PRIVACY COMMISSION

4. Processing necessary to protect **vitally important interests** of the data subject, including his or her life and health;

5. Processing necessary to respond to national emergency or to comply with requirements of **public order and safety**, as prescribed by law.

6. Processing necessary for the fulfillment of a **constitutional or statutory mandate** of a public authority; or

7. Necessary to pursue the **legitimate i of the PIC**, or by a third party r pa whom data is disclosed, except where ... interests are overridden by funda al rights and freedoms of the data subject.



NATIONAL PRIVACY COMMISSION

Processing of Sensitive Personal and Privileged Information (Sec. 13)

1. **Consent** given by data subject, or by the parties to the exchange of privileged information, prior to the processing of such information;

2. Processing is **provided for by existing laws and regulations:** Provided, that the said laws and regulations do not require consent of the data subject for the processing, and guarantee the protection of personal data;

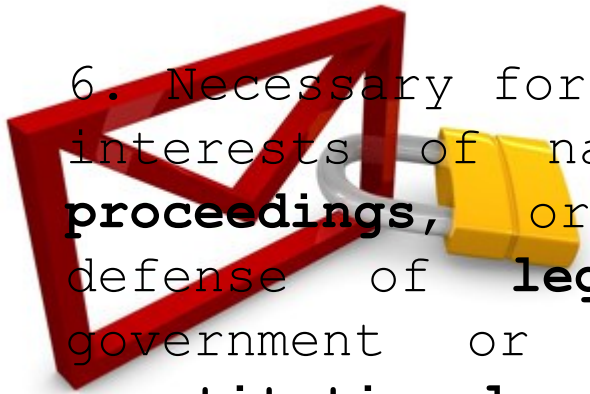
3. Processing **necessary to protect the life and health of the data subject** or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

NATIONAL PRIVACY COMMISSION

4. Processing necessary to achieve the **lawful and noncommercial objectives of public organizations** and their associations provided that:

- Processing is confined and related to the bona fide members of these organizations or their associations;
- SPI are not transferred to third parties;
- Consent of data subject obtained prior to processing

5. Processing necessary for **medical treatment:** Provided, that it is carried out by a medical practitioner or medical treatment institution, and an adequate level of protection of personal data is ensured; or



6. Necessary for the protection of lawful rights and interests of natural or legal persons in **court proceedings,** or the establishment, exercise or defense of **legal c**[illegible] or when provided to government or public [illegible]uthority pursuant to a

NATIONAL PRIVACY COMMISSION

Implementation of Security Measures

Security measures aim to maintain the availability, integrity and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

Technical | Organizational | Physical

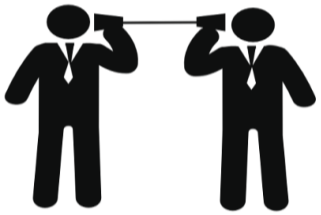
Organizational Security Measures

- Data Protection Policies
  - Amount and extent of processing
  - Storage of personal data
  - Regular review and evaluation of privacy policies and practices
- Records of Processing Activities and Personnel responsible/accessible to such records
- Management of Human Resources
- Procedure and Policies for processing of personal data
- Contracts with Personal Information Processors

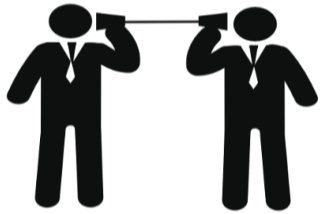

OH NO!
I'M BEING HACKED!
You are being hacked
Haha!
After 10 years of programming, I have finally perfected a program to steal yo-
Wait!
What?!?!
Hacking Failed
@System32Comics
@System32Comics

Physical Security Measures

- Policies and procedures to monitor and limit access to and activities in the workstation or facility
- Design of office space and work stations
- Define duties, responsibilities and schedule of individuals involved in the processing of personal data
- Policies on transfer, removal, disposal and re-use of electronic media
- Procedures that prevent mechanical destruction of files and equipment
- The workstation must be secured against natural disasters, power disturbances, external access and similar threats



NATIONAL PRIVACY COMMISSION



"I CAN ASSURE YOU THAT OUR CONCERN FOR PROTECTING PERSONAL INFORMATION IS VERY DEEP-SEATED!"

NATIONAL PRIVACY COMMISSION

Technical Security Measures

- Security policy with respect to processing of personal data
- Protect computer against accidental, unlawful or unauthorized usage or any interference that will affect data integrity
- Regular monitoring for security breaches and process for identifying and accessing reasonably foreseeable vulnerabilities
- Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Regular testing, assessing and evaluating effectiveness of security measure
- Encryption of personal data during storage, while in transit, authentication process and other technical security measures that control and limit access.

NATIONAL PRIVACY COMMISSION

Privacy Risk Management

Privacy Risk Management

Privacy risk management is a cross-organizational set of processes that helps organizations to understand how their systems, products, and services may create problems for individuals and how to develop effective solutions to manage such risks.

PRIVACY RISK MANAGEMENT

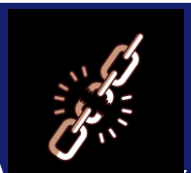
The potential for loss, damage or destruction as a result of a threat exploiting a vulnerability

Ex. Loss of data, alteration, identity theft, unauthorized access, unauthorized disclosure, etc.,

THREAT

A potential cause of an unwanted incident which may result in harm to a system or organization

Ex. Malware, hacking, poor disposal policy, power outage, etc.,



A weakness of an asset or group of asset that can be exploited by one or more threats

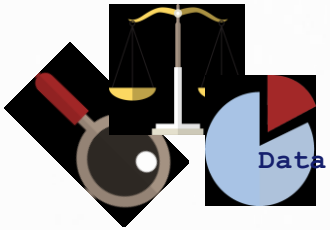
Ex. Software, hardware, employees/individuals, etc.,

A process to evaluate and manage impacts on personal data privacy of a PIC or PIP's programs, projects, process, measure, system or technology product

Guidance on Identifying Privacy Risks

Personal Data Lifecycle
Collection, usage, storage/retention, disclosure, disposal

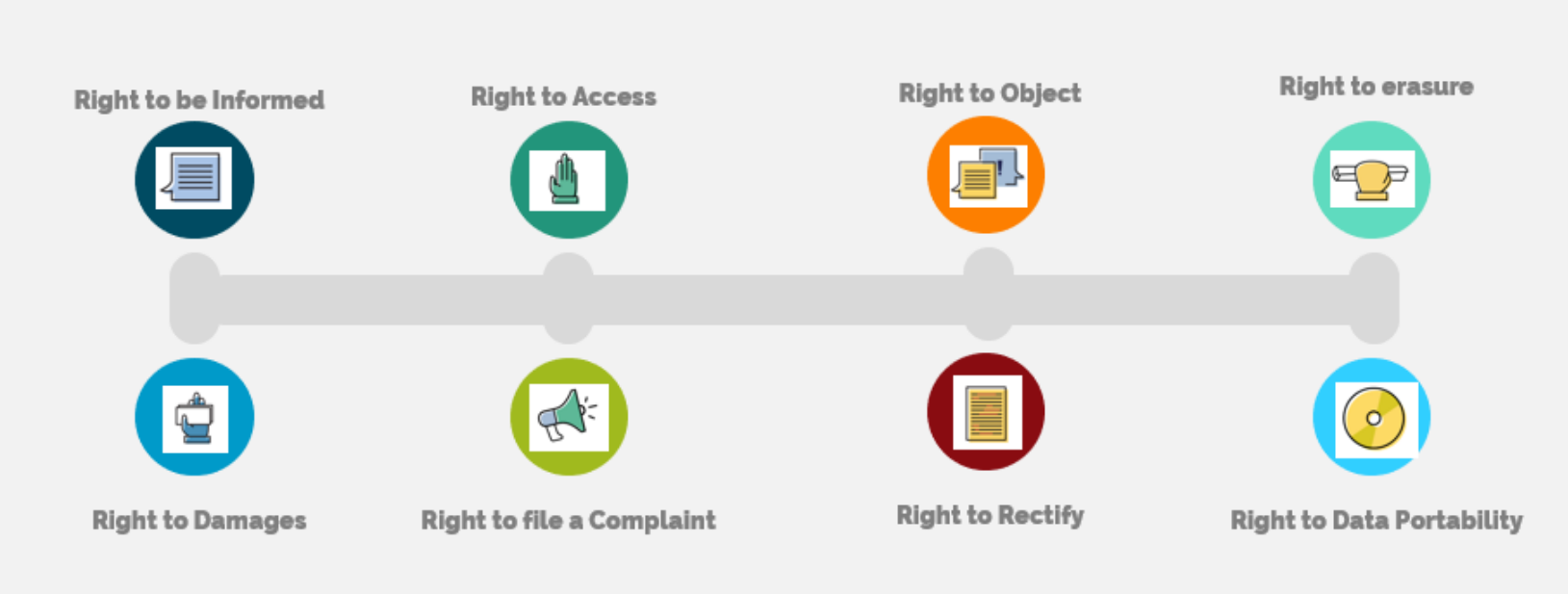
Information Security Principles (C-I-A)



Data Privacy Principles (T-L-P)

Rights of the Data Subjects

Data Subjects' Rights



Rights of Data Subjec

✓Right to **INFORMATION**

WHAT INFORMATION MUST BE SUPPLIED?	WHEN SHOULD INFORMATION BE PROVIDED?
1. Description of the personal data	• before the entry of personal data into the processing system or • at the next practical opportunity
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	

NATIONAL PRIVACY COMMISSION

Rights of Data Subjects

✓Right to **OBJECT**

When does the right to obje apply?

- processing is based on **consent** (includes direct marketing)

- processing is based on **legitimate interest**

NATIONAL PRIVACY COMMISSION

Rights of Data Subje

✓Right to **ACCESS**

Reasonable access to the following:

1. Contents of personal data;

2. Sources of personal data;

3. Names & addresses of recipients of the personal data;

4. Manner by which such

5. Reasons for the disclosure of the personal data, if any;

6. Information on automated processes: where the data will or likely to be made as the sole basis for any decision that significantly affects the data subject;

7. Date when his or her personal data concerning the data subject were last accessed/modified; and

NATIONAL PRIVACY COMMISSION

8. Name and address of the

Rights of Data Subjects

✓Right to **CORRECT OR RECTIFICATION**

- Right to **dispute the inaccuracy or error** in his or her personal data and have the PIC correct it immediately, unless the request is vexatious or otherwise unreasonable.

NATIONAL PRIVACY COMMISSION

Rights of Data Sul

✓Right to **ERASURE OR BLOC**

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

NATIONAL PRIVACY COMMISSION

Rights of Data Subjects

✓Right to **DATA PORTABILITY**

What is this right?

Right to obtain from the PIC a copy of personal data in an electronic/ structured format that is commonly [illegible] further data sub[illegible]

What are the conditions for this right to apply?

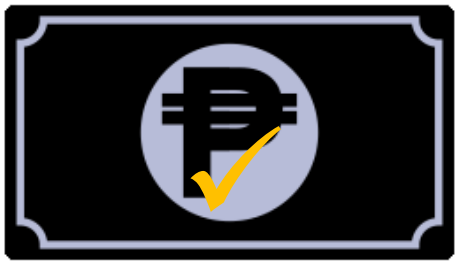
✓personal data requested concerns the data subject making the request;
✓personal data is processed electronically; and
✓processing is based on consent or contract.

NATIONAL PRIVACY COMMISSION

Rights of Data Subjects

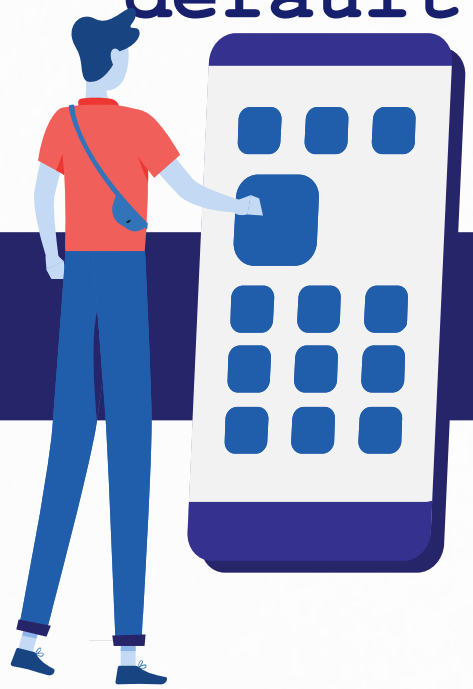
✓Right to **FILE A COMPLAINT AND TO DAMAG**

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.



NATIONAL PRIVACY COMMISSION

Privacy-by-design & privacy-by-default



Privacy-by-design

Data protection through technology design. A systematic approach wherein privacy is embedded within the system development lifecycle

Privacy-by-default

Once a product or service has been released to the public, the strictest privacy setting should apply by default

Data Breach Management

What is Data Breach Management?

It is the process of identifying, managing, recording and analyzing information security threats or incidents affecting personal data and its management.

Be prepared for Security Incidents

Security Incident Management and Personal Data Breach Reporting Procedure

Availability Breach — loss, accidental or unlawful destruction of personal data.

Integrity Breach — alteration of or unauthorized changes to personal data.

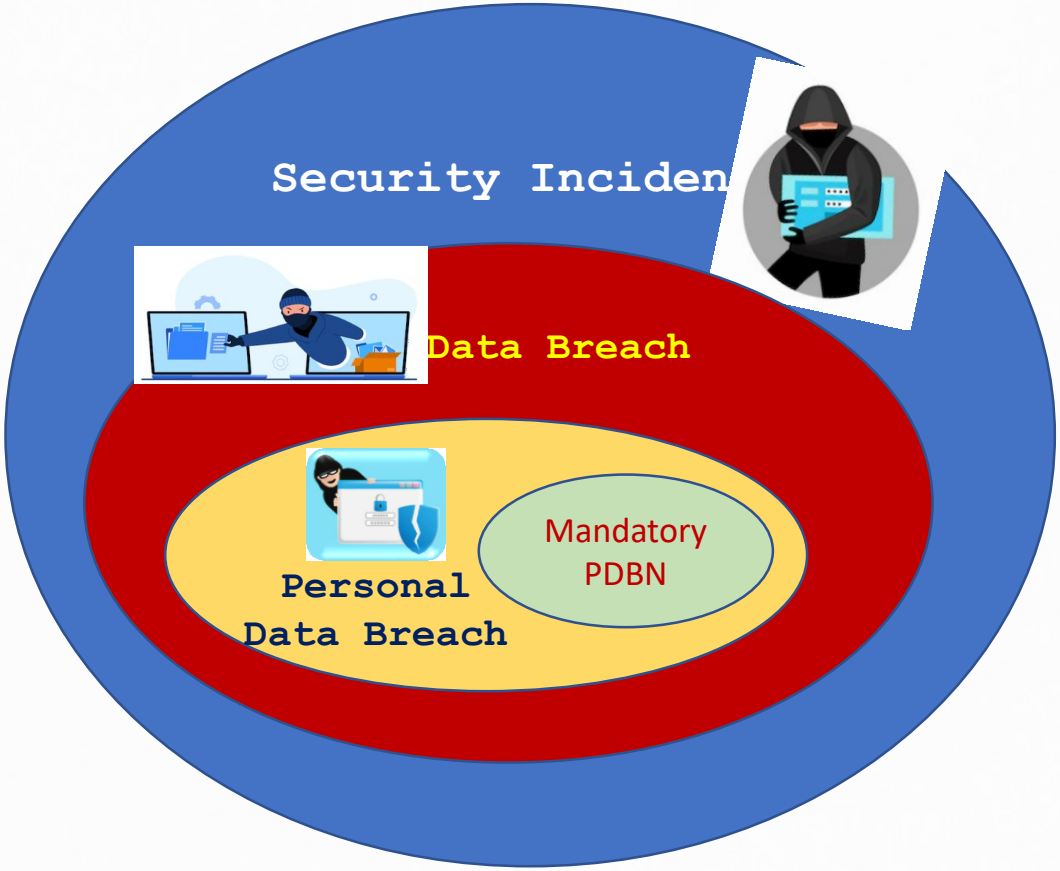
Confidentiality Breach — unauthorized disclosure of or access to personal data.

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.

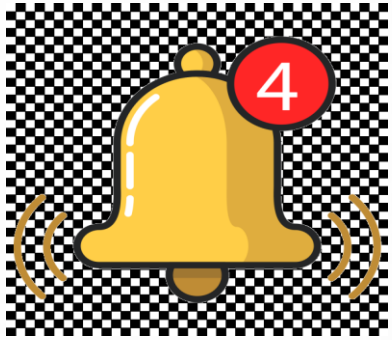
A **security incident** is an event or situation that affects or will likely affect data protection or compromise the availability, integrity, and confidentiality of personal data.

All personal data breaches are essentially security incidents.

A security incident will result in a personal data breach if there are no existing safeguards to remedy the situation.


Security Incident
Data Breach
Personal
Data Breach
Mandatory
PDBN

When is Notification required?

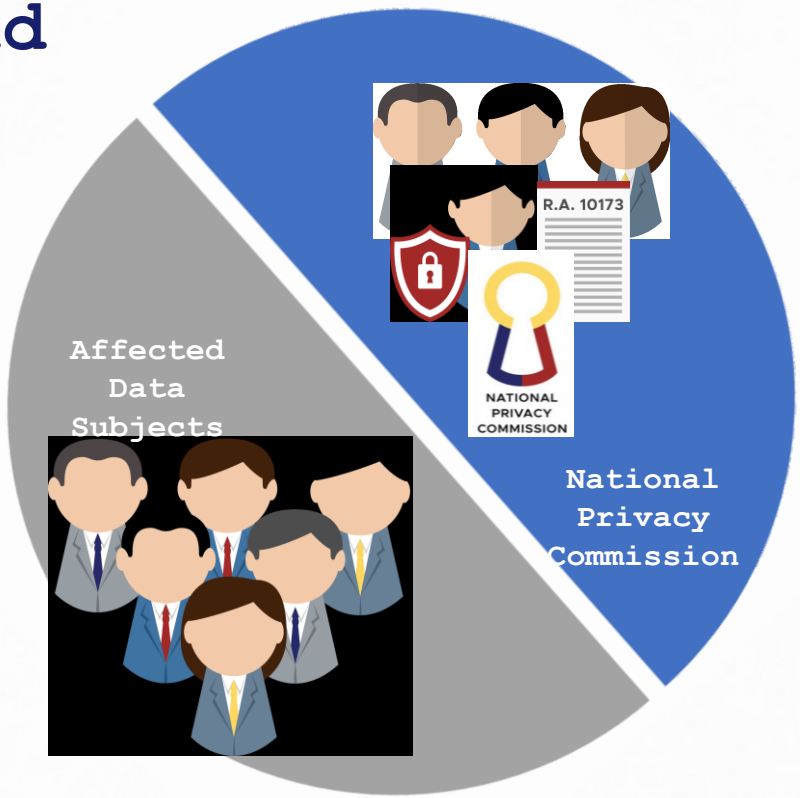


Notification of a data breach is mandatory when:

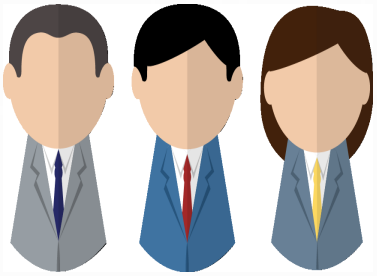
1. The personal data involves:
   - **sensitive personal information** or
   - any **other information** that may be **used to enable identity fraud;**
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

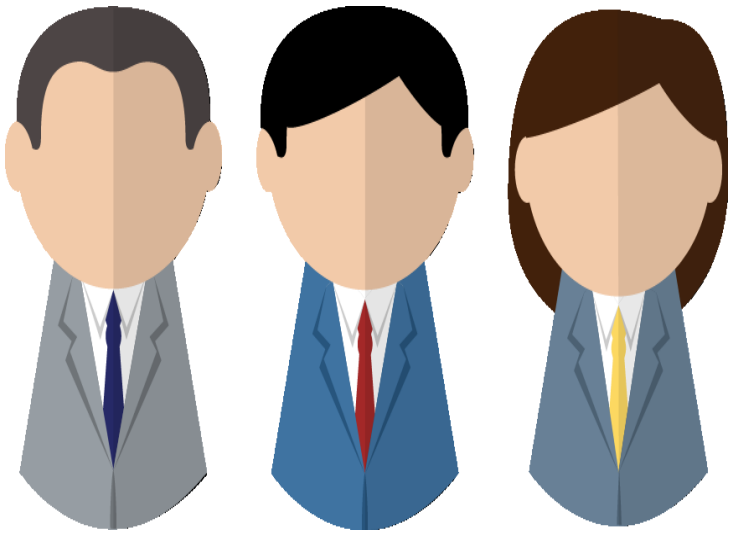
Who Should Notify and Who Should be Notified?

The obligation to notify remains with the Personal Information Controller even if the processing of information is outsourced or subcontracted to a Personal Information Processor.



Guidelines for Personal Data Breach Management





- ✓ **Creation of a data breach response team**, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach.

- ✓ **Implementation of security measures** and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident.

- ✓ **Implementation of an incident response procedure** intended to contain a security incident or personal data breach and restore integrity to the information and communications system.

- ✓ **Mitigation of possible harm and negative consequences** to a data subject in the event of a personal data breach; and

Obligations of a Personal Information Controller

The PIC should collect personal information only for specified and legitimate purposes

The PIC should process personal information fairly and lawfully.

The PIC should process accurate, relevant and up to date personal information.

The PIC should collect and process personal information adequately and not excessively.

The PIC should retain personal information only for as long as necessary

The PIC must implement reasonable organizational, physical, technical security measures to protect personal data.

NATIONAL PRIVACY COMMISSION

ABS-CBN NEWS

Share

Over 900,000 affected by Cebuana Lhuillier data breach

Arianne Merez, ABS-CBN News

Posted at Jan 19 2019 12:55 PM | Updated as of Jan 19 2019 07:29 PM

MANILA (2nd UPDATE)—More than 900,000 clients of Cebuana Lhuillier were affected by a breach that may have compromised their personal data, the local pawnshop said Saturday.

The figure represents about 3 percent of its total clientele, Cebuana Lhuillier said.

Information that could have been compromised includes birth dates, addresses, and sources of income, the company said in a statement.

Cebuana Lhuillier bares data breach, tells clients to secure accounts

It, however, noted that transaction details or information were not compromised and that the pawnshop's main servers "remain safe and protected."

P.J. LHUILLIER
GROUP OF COMPANIES

SECTIONS Friday, July 19, 2019 INQUIRER.NET TODAY'S PAPER

Jollibee ordered to suspend online delivery system over privacy concern

NPC: PRIVACY OF 18M PEOPLE IN FASTFOOD CHAIN'S DATABASE IN HIGH RISK

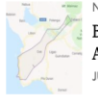
By: Roy Stephen C. Canivel - @inquirerdotnet 08:27 PM May 08, 2018

Click to listen now
01:58 Powered by Trinity Audio

LATEST STORIES MOST READ

NEWSINFO
At least 11 pupils killed as dump truck falls into cliff in Cebu town
JULY 19, 2019 10:51 AM

NEWSINFO
LIST: Manila public viewing sites of Pacquiao, Thurman bout on July 21
JULY 19, 2019 10:36 AM



NEWSINFO
British national drowns in Albay resort
JULY 19, 2019 10:28 AM

NEWSINFO

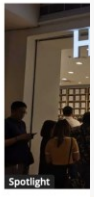
BusinessWorld 30°c CEBU CITY

Cebu Pacific says GetGo app server compromised

April 26, 2019 | 12:02 am

Font Size A A A

SPOTL



SECTIONS Friday, July 19, 2019 INQUIRER.NET TODAY'S PAPER

Data leak hits Wendy's Philippines database

FOOD FIRM ORDERED TO NOTIFY PEOPLE WHOSE RECORDS HAD BEEN EXPOSED

By: Roy Stephen C. Canivel - @inquirerdotnet Inquirer Business / 08:11 PM May 04, 2018

Click to listen now
01:32 Powered by Trinity Audio

LATEST STORIES MOST READ

NEWSINFO
At least 11 pupils killed as dump truck falls into cliff in Cebu town
JULY 19, 2019 10:51 AM

NEWSINFO
LIST: Manila public viewing sites of Pacquiao, Thurman bout on July 21
JULY 19, 2019 10:36 AM

NEWSINFO
British national drowns in Albay resort

10 Pointers to Substantial Compliance

1. Organizational Governance

   For Government Sector, create a centralized organizational structure for Data Privacy in the Organization (Section 10 Cir 22-01)
   a. Policy should be Top to Bottom
   b. Reporting should be Bottom to Top

   For the Private Sector, create an effective and efficient organizational structure that will ensure policy, reporting and review mechanisms for the advancement of personal data privacy and data protection (Centralized, Decentralized, Hybrid)

2. Conduct a Privacy Impact Assessment of ALL Processes and Data Processing Systems that process personal data.
3. Create your Privacy Management Program
4. Implement a Central Privacy Manual for the whole Organization
5. Register your DPO, COPs and All Data Processing Systems with the Commission through the NPC Registration System (NPCRS)
6. Create a Data Breach Response Team / Security Incident Management Team
7. Practice the reporting procedures for Personal Data Breach for Mandatory notification and Annual Security Incident Reporting through the Data Breach Notification and Management System (DBNMS).
8. Implement Organizational, Technical, and Physical Security Measures to Protect the Confidentiality, Integrity and Availability of Personal Data
9. Create mechanisms for data subjects to exercise ALL the eight (8) data subject rights.
10. Adhere to the three principles of Data Privacy
    a. Legitimate Purpose - Lawful Basis of Processing (Section 12 and 13 DPA)
    b. Transparency - Go Public with a Privacy Statement and ensure Privacy Notices exist per process or data processing system
    c. Proportionality - Process only what is necessary to provide complete public service

Guidelines in Data Processing System (DPS) Registration

Personal Information Controller / Personal Information Processor

1 ACCOUNT CREATION

Access the National Privacy Commission Registration System [NPCRS] at **https://npcregistration.privacy.gov.ph**

Upon signing up, the PIC or PIP shall input the name and contact details of the Data Protection Officer (DPO) together with a unique and dedicated email address, specific to the position of DPO. [*Official DPO Email]

NOTE: ***All are required to use an Official DPO email address, not personally identified with the person of the appointed DPO but with the position of DPO.***
(i.e. dataprotection@domain.com)

REGISTRATION PROPER 2

LOGIN USING CREDENTIAL

- Select Type of DPO/DPS Registration
- During registration proper, the PIC or PIP shall:

a. Encode the organizational details; name and contact details of the Head of the Organization or Head of Agency.
b. Encode Data Processing System(s) details, all Data Processing System of the PIC or PIP at the time of initial registration.
c. Click "Save Registration".
d. Encode the details of Compliance Officer(s) for Privacy if applicable.
e. Upload the prescribed supporting documents as provided under Section 11, NPC Circular No. 22-04.

1. For government agencies: Special or Office Order, or any similar document, designating or appointing the DPO of the PIC or PIP;

2. For domestic private entities:

1. For Corporations:
a) (1) duly notarized Secretary's Certificate authorizing the appointment or designation of DPO, or
(2) any other document demonstrating the validity of the appointment or designation of the DPO signed by the Head of the Organization with an accompanying valid document conferring authority to the Head of Organization to designate or appoint persons to positions in the organization.
b) Securities and Exchange Commission (SEC) Certificate of Registration.
c) certified true copy of latest General Information Sheet.
d) valid business permit.

2. For One Person Corporation:
a) (1) duly notarized Secretary's Certificate authorizing the appointment or designation of DPO, or (2) any other document that demonstrates the validity of the appointment or designation of DPO signed by the sole director of the One Person Corporation.
b) SEC Certificate of Registration
c) valid business permit.

3. For Partnerships:
a) duly notarized Partnership Resolution or Special Power of Attorney authorizing the appointment or designation of DPO, or any other document that demonstrates the validity of the appointment or designation.
b) SEC Certificate of Registration.
c) valid business permit.

4. Sole Proprietorships:
a) duly notarized document appointing the DPO and signed by the sole proprietor, in case the same should elect to appoint or designate another person as DPO.
b) DTI Certificate of Registration.
c) valid business permit.

5. For foreign private entities:
1. Authenticated copy or Apostille of Secretary's Certificate authorizing the appointment or designation of DPO, or any other document that demonstrates the appointment or designation, with an English translation thereof if in a language other than English.
2. Authenticated copy or Apostille of the following documents, with an English translation thereof if in a language other than English, where applicable:
a) Latest General Information Sheet or any similar document.
b) Registration Certificate (Corporation, Partnership, Sole Proprietorship) or any similar document.
c) valid business permit or any similar document.

FOR NOTARIZATION

a. Export DPO Form (PDF format) automatically created during DPS registration.
b. Print and Sign downloaded form (both DPO and Head of the Organization or Agency).
c. Have the filled-out form notarized.
d. Scan, upload and submit notarized DPO Form.

NOTE: The submissions of the PIC or PIP shall undergo review and validation by the Commission. In case of any deficiency, the PIC or PIP shall be informed of the same and shall be given five (5) days to submit the necessary requirements.

3 DOWNLOAD CERTIFICATE OF REGISTRATION AND NPC SEAL OF REGISTRATION

Once the submissions have been validated and considered complete, the PIC or PIP shall be informed that the Certificate of Registration together with the NPC Seal of Registration is available for download.

NOTE: To generate the Certificate of Registration and Seal of Registration, disable the pop-up blockers and allow multiple downloads in the browser.

NPCRS Video Demo

FOR REFERENCE

NPCRS Video Demo: privacy.gov.ph/wp-content/uploads/2023/05/NPCRS-Demo.mp4
Frequently Asked Questions (FAQs):
https://privacy.gov.ph/pips-and-pics/faqs/

For inquiries email us at:

DPS Registration – registrationsupport@privacy.gov.ph
NPCRS Concerns – adminnpcrs@privacy.gov.ph

Contact us:

Trunkline: +632 5322 – 1322 local 103/118
Smart: 09101029114
Globe: 09652863419

BAGONG PILIPINAS
NATIONAL PRIVACY COMMISSION
ISO 9001:2015 CERTIFIED
SOCOTEC

Thank you!

Email us at
info@privacy.gov.ph
compliancesupport@privacy.gov.ph
complaints@privacy.gov.ph

Visit us at:
https://www.privacy.gov.ph

Your feedback is important to us. Please scan or access through https://forms.office.com/r/6payUueNSD

Speaker name: Atty. Anna Benjieline R. Puzon
Topic: Managing Data Privacy Risks and Maintaining Regulatory Compliance