

The Data Privacy Act of 2012

Impact and Significance

To non-life INSURANCE SECTOR

RAYMUND ENRIQUEZ LIBORO
PRIVACY COMMISSIONER AND CHAIRMAN

2016 – Awareness

2017 – Compliance

2018 – Enforcement

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

RESILIENCE AND THE FILIPINO SPIRIT



RESILIENCE AND THE FILIPINO SPIRIT

May 27, 2010

REPUBLIC ACT NO. 10121

AN ACT STRENGTHENING THE PHILIPPINE DISASTER RISK REDUCTION AND MANAGEMENT SYSTEM, PROVIDING FOR THE NATIONAL DISASTER RISK REDUCTION AND MANAGEMENT FRAMEWORK AND INSTITUTIONALIZING THE NATIONAL DISASTER RISK REDUCTION AND MANAGEMENT PLAN, APPROPRIATING FUNDS THEREFOR AND FOR OTHER PURPOSES

SECTION 1. *Title.* — This Act shall be known as the "Philippine Disaster Risk Reduction and Management Act of 2010".

SECTION 2. *Declaration of Policy.* — It shall be the policy of the State to:

- (a) Uphold the people's constitutional rights to life and property by addressing the root causes of vulnerabilities to disasters, strengthening the country's institutional capacity for disaster risk reduction and management and building the resilience of local communities to disasters including climate change impacts;

RESILIENCE AND THE FILIPINO SPIRIT



Resilience



- **Resilience**
- **rɪˈzɪljəns/**
- **noun**
 - **1.the capacity to recover quickly from difficulties; toughness.**
 - **adapt well to change**
 - **keep going in the face of adversity**

21st Century Hazards and Risks



Norse – Superior Attack Intelligence

Norse maintains the world's largest dedicated threat intelligence network. With over eight million sensors that emulate over six thousand applications – from Apple laptops, to ATM machines, to critical infrastructure systems, to closed-circuit TV cameras – the Norse Intelligence Network gathers data on who the attackers are and what they're after. Norse delivers that data through the Norse Appliance, which pre-emptively blocks attacks and improves your overall security ROI, and the Norse Intelligence Service, which provides professional continuous threat monitoring for large networks.

LIVE ATTACKS						
Timestamp	Attacker	Attacker IP	Attacker Geo	Target Geo	Attack Type	Port
14:56:21.719	Microsoft Corporation	207.46.100.252	Redmond, US	De Kalb Junction, US	smtp	25
14:56:21.284	This Ip Network Is Used For Internet Security Research. Int	185.35.62.250	Geneve, CH	Dubai, AE	ntp	123
14:56:20.770	Philippine Long Distance Telephone Company	122.3.47.120	Paranaque, PH	Lynnwood, US	telnet	23
14:56:20.580	Microsoft Corporation	65.55.169.249	Washington, US	De Kalb Junction, US	smtp	25
15:05:41.557	Philippine Long Distance Telephone Company	122.54.132.220	Makati, PH	Dubai, AE	telnet	23
15:19:19.784	Microsoft Corporation	207.46.100.250	Redmond, US	De Kalb Junction, US	smtp	25
15:04:02.333	Philippine Long Distance Telephone Company	122.3.47.120	Paranaque, PH	Lynnwood, US	telnet	23

PROF

The Data Privacy Act of 2012



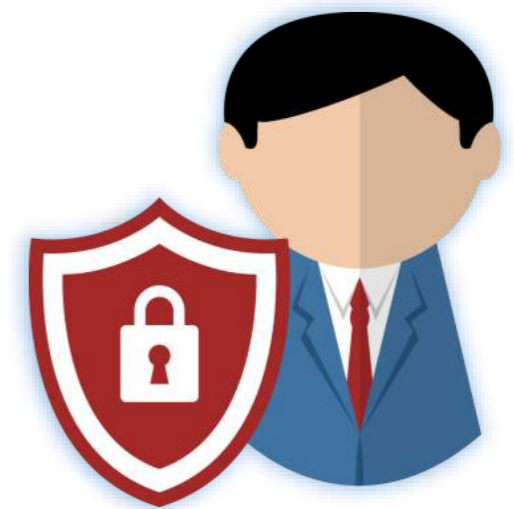
A 21st Century Law

**For 21st Century
Rights and Risks**

PROPER

What is a Privacy Risk?

*A Personal Data Breach
or a Data Privacy
Violation that has NOT
happened yet.*



P

What is Privacy Resilience?

**A Personal Data Breach or
a Data Privacy Violation
that was prevented.**

**A breach and privacy
disaster that
did not happen.**

COMMISSION



Disaster



Resilience





DPA and the Philippine Development Plan



www.clipartsuggest.com/four-pillars-cliparts/



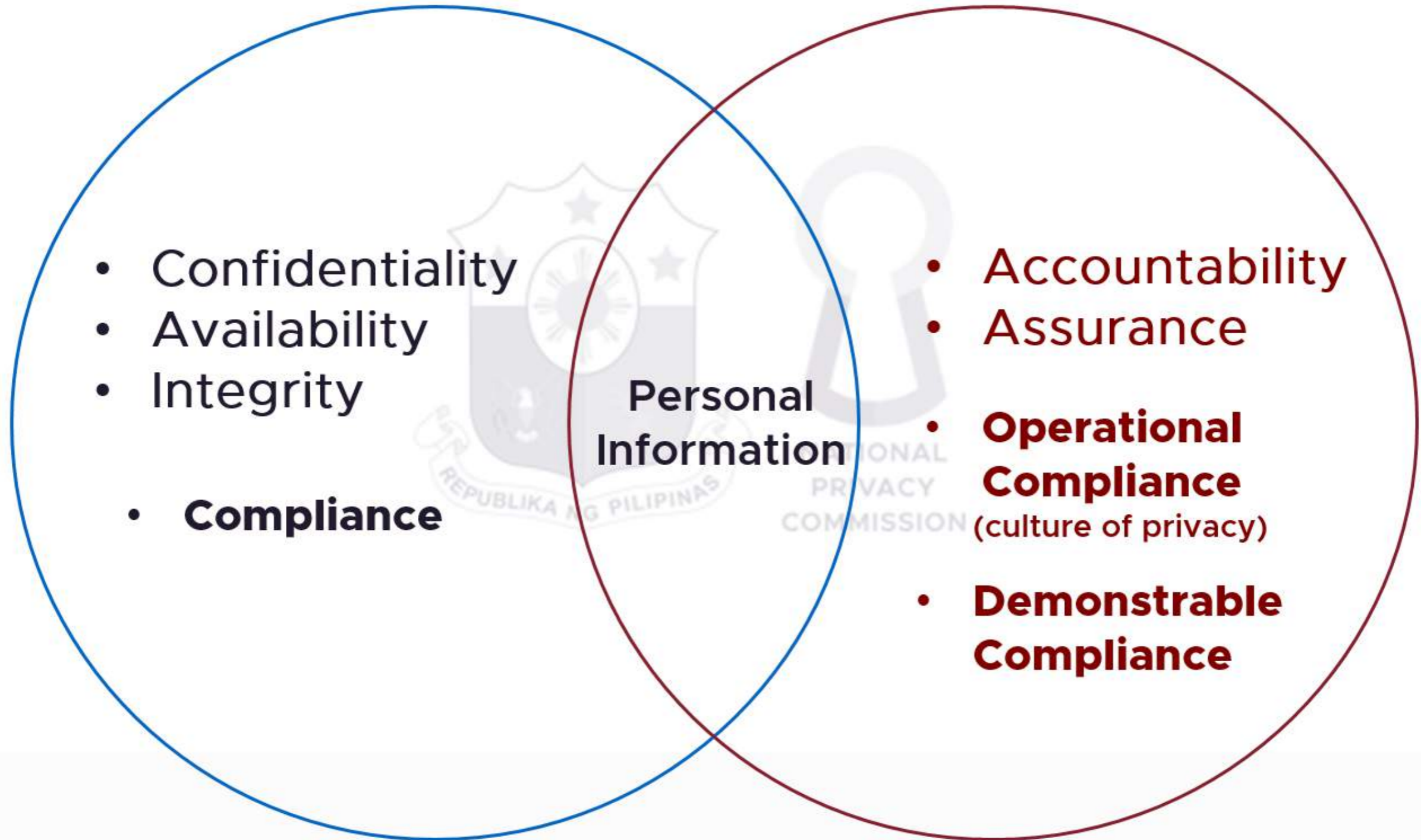
THE PRIVACY COMMISSIONER

Philosophy

Risk management approach | Prevention and mitigation | Building the culture of data privacy and protection

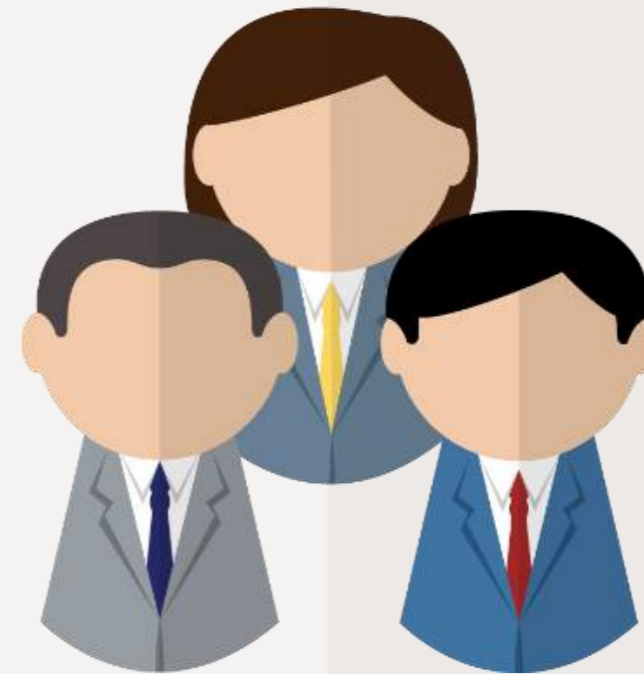
Data Protection

Data Privacy



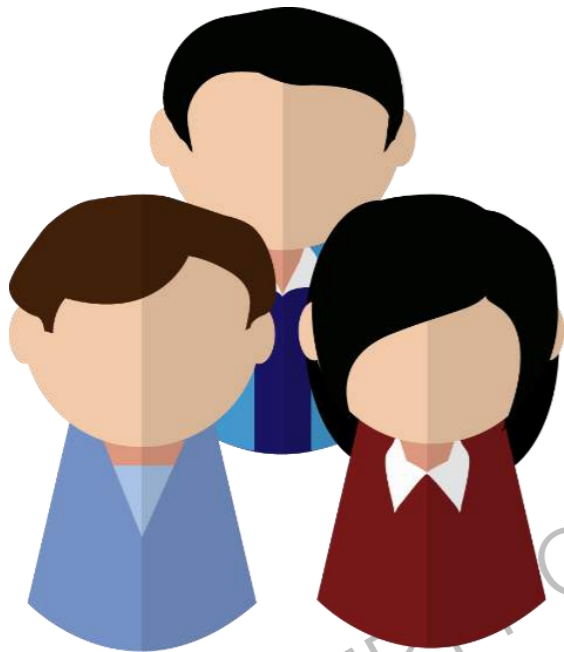


**What the law is
all about**



**How it will
affect you**

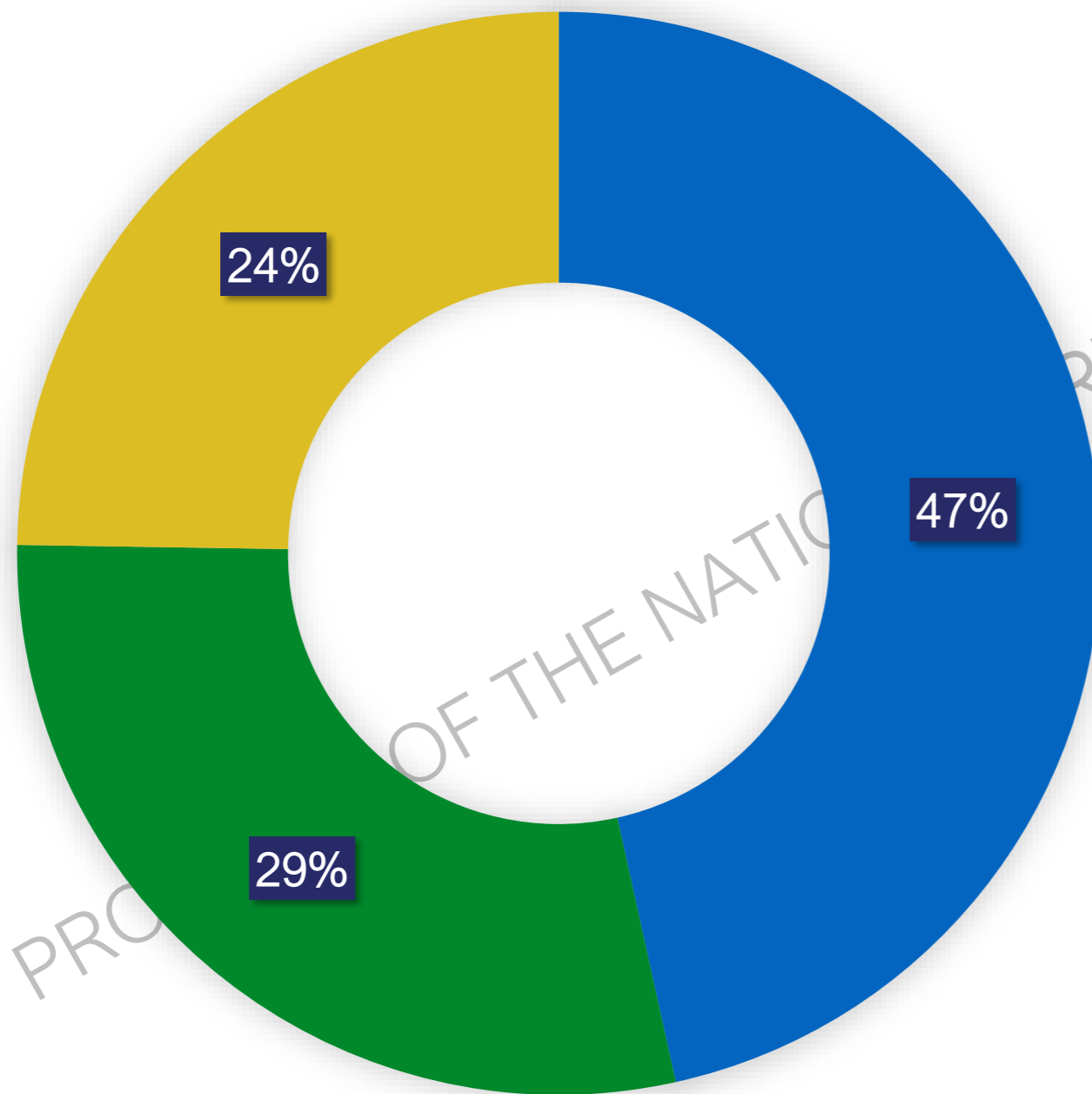
Impact of a Problematic Data Action on Business



- **Loss of reputation**
- **Loss of market share**
- **Legal liabilities**

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

ROOT CAUSES OF BREACH



■ **Malicious or criminal attack**

■ **System Glitch**

■ **Human Error**

HOW DO PRIVACY BREACHES OCCUR

Insurance Company Fined \$6.8 Million for Data Breach

The fine is in response to the exposure of data belonging to 13,336 of TSS' Dual Eligible Medicare beneficiaries.

On September 20, 2013, TSS mailed a pamphlet to approximately 70,000 Medicare Advantage beneficiaries that inadvertently showed some recipients' Medicare Health Insurance Claim Numbers, which are considered protected health information under the Health Insurance Portability and Accountability Act ([HIPAA](#)).

Following the discovery of the error, TSS reported the incident to state and federal authorities, notified affected beneficiaries, and offered all those affected 12 months of free credit monitoring services.

"We take this matter very seriously and are working to prevent this type of incident from recurring," TSS Management stated in a [recent SEC filing](#) regarding the fine.

In addition to the fine, all new enrollments of Dual Eligible Medicare beneficiaries who were affected will be offered the option to disenroll.

Photo courtesy of Shutterstock.

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

HOW DO PRIVACY BREACHES OCCUR

Large Insurance Company Settles for \$5.5 Million over "Failed To Patch" Data Breach

Stu Sjouwerman

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

de) agreed to pay a total of \$5.5 Million to resulting from the loss of critical consumer data breach.

ent, the respondent lost the data for 1.27 when hackers exploited a security breach to implement a security patch.

ice company agreed to appoint a security patch policies and procedures, and perform

criticized the respondent for its "true carelessness while collecting and retaining users, needlessly exposing their personal data in the process."



Nationwide®

<https://blog.knowbe4.com/large-insurance-company-settles-for-5.5-million-over-failed-to-patch-data-breach>

HOW DO PRIVACY BREACHES OCCUR

AXA data breach affects 5,400 Singapore customers

🕒 PUBLISHED SEP 7, 2017, 4:49 PM SGT | UPDATED SEP 7, 2017, 10:04 PM

BRANDED CONTENT

SINGAPORE - The personal data of 5,400 customers of AXA Insurance in Singapore was stolen due to a cyber attack.

The life insurance firm sent out an e-mail to most affected customers on Thursday, notifying them of the data breach. The remaining affected customers will be notified on Friday (Sept 8).

In the e-mail, AXA's data protection officer Eric Lelyon said: "We wish to inform you because of a recent cyber attack, personal data belonging to about 5,400 of our past and present, on our Health Portal was compromised."

<http://www.straittimes.com/singapore/axa-data-breach-affects-5400-singapore-customers>

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

DATA PRIVACY RELATED DIFFICULTIES



- Customer database breaches
- Company's lack of adequate policies to protect customer information
- Payment card security breaches
- Customer profiling leading to transparency concerns

PROCESSING PERSONAL INFORMATION CAN CREATE PROBLEMS FOR INDIVIDUALS



- Loss of trust
- Loss of self-determination
 - *Loss of autonomy*
 - *Loss of liberty*
 - *Exclusion*
 - *Physical harm*
- Discrimination
 - *Stigmatization*
 - *Power imbalance*
- Economic loss



**NATIONAL
PRIVACY
COMMISSION**



AN

introduction

TO THE


Data Privacy Act

OF 2012



FULL TITLE

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



Where
is **privacy** in
all of these?

FULL TITLE

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***

STRUCTURE OF RA 10173



Sections 1-6.
Definitions and
General Provisions
.....

Sections 25-37.
Penalties
.....

Sections 7-10.
The National
Privacy
Commission
.....

Sections 22-24.
Provisions
Specific
to Government
.....



Sections 11-21.
Rights of Data Subjects, and Obligations of
Personal Information Controllers and Processors
.....

PROPERTY OF THE

COMMISSION

THE SCOPE AND POLICY OF



THE DATA PRIVACY ACT OF 2012

The Privacy Ecosystem



POLICY



SEC. 2. Protect the **fundamental human right of privacy** of communication while ensuring **free flow of information to promote innovation and growth**; role of information and communications technology to ensure that **personal information under the custody of the government and private sector are secured.**

PROPER

TIONAL PRIVACY COMMISSION

BALANCE

Data Privacy

Free Flow

Information Privacy

Research

National Security and Public Safety

Right to Information

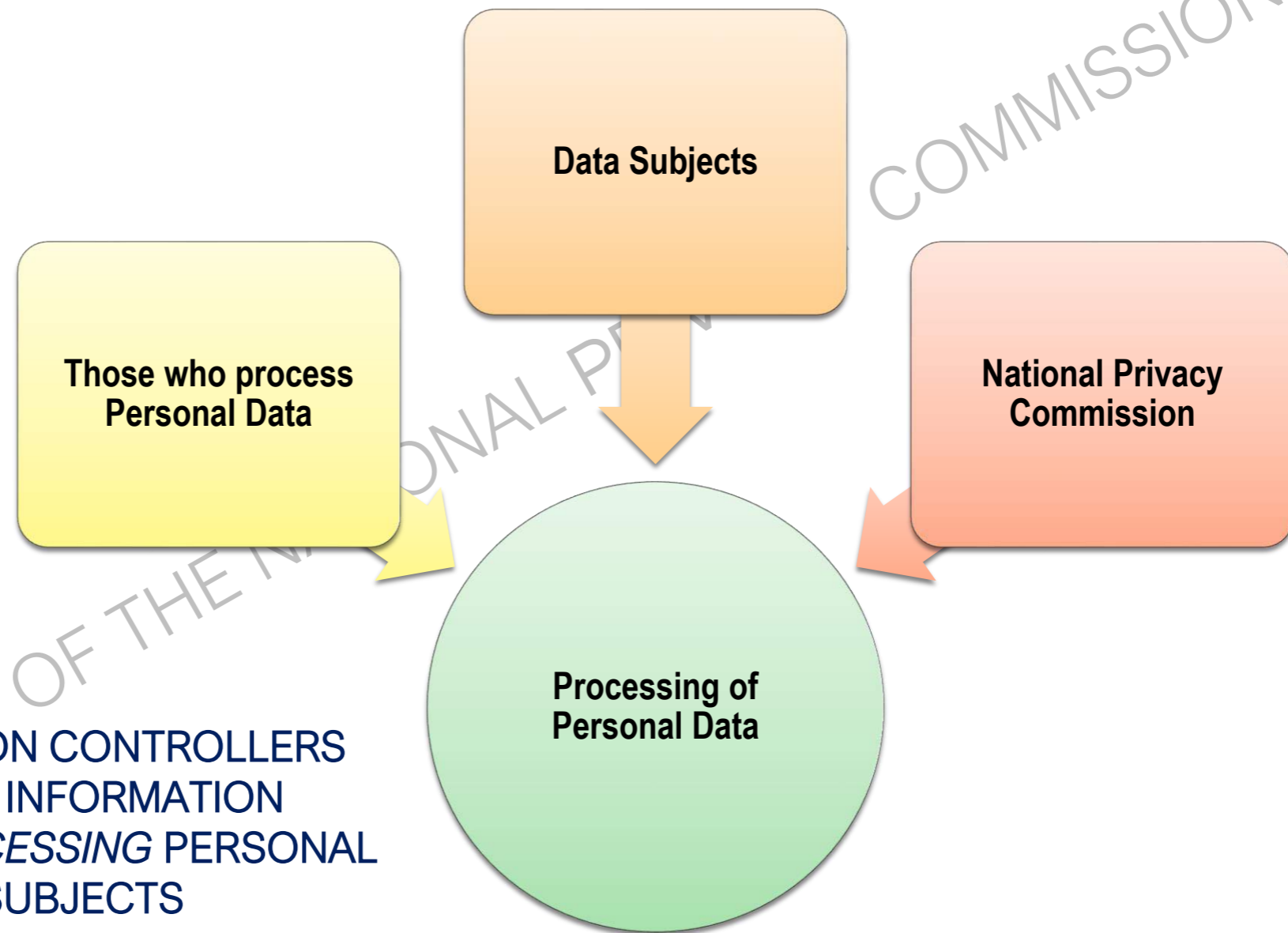
National Privacy Commission

SCOPE

- ✂ **SEC. 4.** Applies to the **processing of all types of personal information**, in the country and even abroad, subject to certain qualifications.
- ✂ **SEC. 15.** Personal information controllers may invoke the **principle of privileged communication** over privileged information that they lawfully control or process.



SCOPE OF THE LAW



- PERSONAL INFORMATION CONTROLLERS (PIC) and PERSONAL INFORMATION PROCESSORS (PIP) PROCESSING PERSONAL DATA of DATA SUBJECTS

PROCESSING

Any operation of 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.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

**CREATE AND
COLLECT**



**STORE AND
TRANSMIT**



**DISPOSE
AND
DESTROY**



THE DATA LIFE CYCLE

RETAIN



**USE AND
DISTRIBUTE**



PROPERTY OF THE NATIONAL PRIVACY COMMISSION

OBLIGATIONS OF A PERSONAL INFORMATION CONTROLLER



The PIC should collect personal information for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection



The PIC should process personal information fairly and lawfully, and in accordance with the rights of a data subject.



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 for the fulfillment of the purposes for which the data was obtained. The information should be kept in a form which permits identification of data subjects for no longer than is necessary.



The PIC must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information.



Transparency

Legitimate Purpose

Proportionality

Security

Accountability

Choice

Notice

Access

Remedy



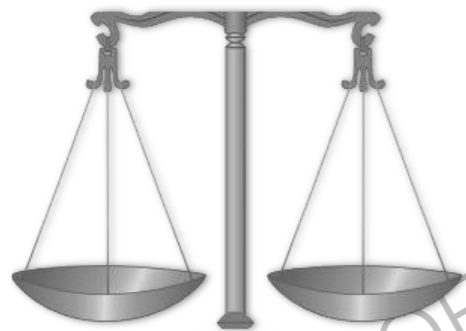
IvyDPatdvc

DATA PRIVACY PRINCIPLES

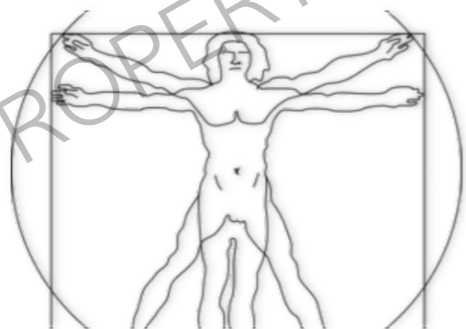
DP
FOR NON-LIFE INSURANCE



TRANSPARENCY



LEGITIMATE PURPOSE



PROPORTIONALITY

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

TRANSPARENCY



Principle of 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.

LEGITIMATE PURPOSE



Principle of 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



Principle of 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.

“PROPORTIONALITY”

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

Pr



Ninja Pepe

Like This Page · February 8 · Edited ·

THE FIVE

Pillars

OF

Compliance

PROPERTY OF THE NATIONAL PRIVACY COMMISSION





Commit to Comply:
Appoint a **Data Protection Officer** (DPO).



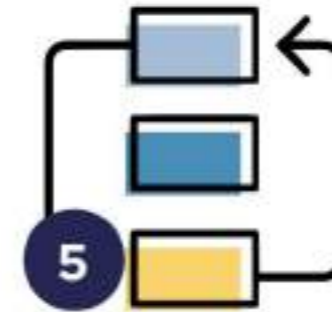
Know Your Risks:
Conduct a **Privacy Impact Assessment** (PIA).




Be Accountable:
Create your **Privacy Management Program** and **Privacy Manual**.



Demonstrate Your Compliance: Implement your **privacy and data protection** (PDP) measures.



Be Prepared for Breach: Regularly exercise your **Breach Reporting Procedures** (BRP).



When will you hear from the NPC?

1. When the NPC sends **advisories and circulars**
2. When the NPC **conducts audit and compliance checks**
3. When you **notify the NPC about a personal data breach**

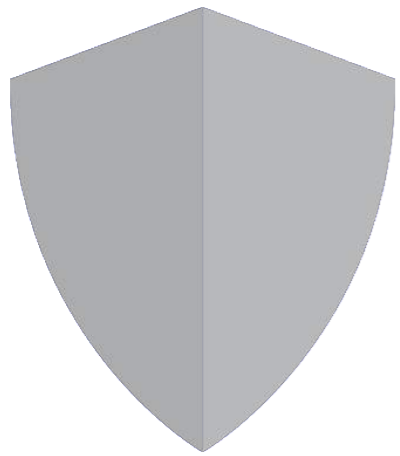
What do we look for when the NPC comes knocking at your door?



1. Can we feel a culture of **Privacy**?
2. Do you have a **sensible data privacy program**?
3. Is it based on **risk assessment**?
4. Do you **train your staff in data privacy** and protection?
5. Are you prepared for **breach**?

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

The Data Privacy Golden Rule

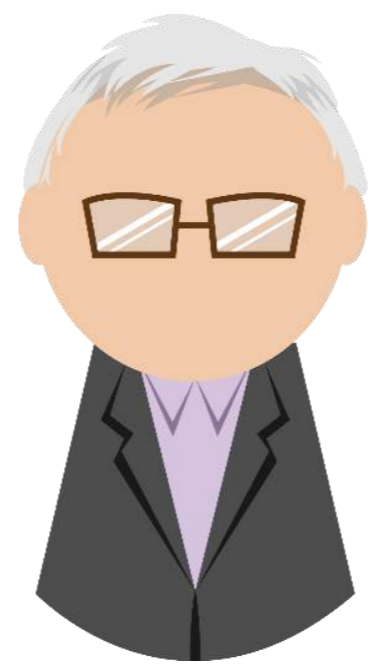


If you Can't Protect It...

DONT Collect It.



PROPERTY OF THE NATIONAL PRIVACY COMMISSION



PRIVACY.GOV.PH

facebook.com/privacy.gov.ph
twitter.com/privacyph
info@privacy.gov.ph



PROPERTY OF THE NATIONAL PRIVACY COMMISSION