

# Overview of the Data Privacy Act of 2012

**National Privacy Commission**



What the **law** is  
all about



How it will  
affect **you**

# 1995

# DP



# 15

NON-BANK FINANCIAL INSTITUTIONS



Picture from <http://www.rappler.com/specials/pope-francis-ph/80492-pope-john-paul-assassination-plot>



# 2015

# DP



# 15

NON-BANK FINANCIAL INSTITUTIONS



Picture from <http://dzhnews.com.ph/pope-silent-upon-hearing-stories-yolanda-victims/>



# DATA IS THE NEW OIL OF THE DIGITAL ECONOMY



PROPERTY OF NATIONAL PRIVACY COMMISSION



## 2007



Exxon Mobil



Petrochina



General Electric



China Mobile



ICBC



Microsoft



Royal Dutch



Gazprom



AT&T

## 2017



Apple



Google



Microsoft



Facebook



Coca Cola



Amazon



Disney



Toyota



McDonalds



Samsung

**Forbes  
Most  
Valuable  
Brands**

D P

NON-BANK FINANCIAL INSTITUTIONS



15

The world's largest taxi company, owns **no vehicles**.

The world's most popular media owner, creates **no content**.

The world's most valuable retailer, has **no inventory**.

The world's largest accommodation provider, owns **no real estate**.



UBER



FACEBOOK



ALIBABA



AIRBNB

PROPERTY OF NATIONAL PRIVACY COMMISSION



**1998:** Yahoo refuses to buy Google for \$1 million.

**2002:** Yahoo realizes its mistake and tries to buy Google for \$3 billion. Google says "Give us \$5 billion", Yahoo says no.

**2008:** Yahoo refuses to be sold to Microsoft for \$40 billion dollars.

**2016:** Yahoo sold for \$4.6 billion to Verizon.



# ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select ▾

[See Your Matches »](#)

Over **37,565,000** anonymous members!



**As seen on:** Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

**Ashley Madison** is the world's leading married dating service for **discreet** encounters



Trusted Security Award



SSL Secure Site

Over **39,470,000** anonymous members!

# ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

See your Match

Over 37,655,000 anonymous members!





# Ashley Madison let off with \$1.66m fine over huge hack

Customers receive nothing from settlement with US Federal Trade Commission, which decided owner Ruby Corp was unable to pay full \$17.5m penalty

This article is 9 months old

55 60  
Reuters in Toronto

Thursday 15 December 2016 01:40 GMT



Regulators suspended most of Ashley Madison's \$17.5m fine because they were not 'looking to put a company out of business'. Photograph: Philippe L'Orange/Getty Images

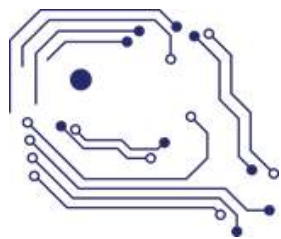
The owner of hacked infidelity website **Ashley Madison** will pay a sharply discounted \$1.66m penalty to settle US investigations into lax data security and deceptive practices.

The remainder of a \$17.5m settlement was suspended based on privately held Ruby Corp's inability to pay.

"I recognise that it was a far lower number frankly than I would have liked," said Federal Trade Commission chairwoman Edith Ramirez. "We want them to feel the pain. We don't want them to profit from unlawful conduct. At the same time we are not going to seek to put a company out of business."

The size of the payment means Ashley Madison's customers will not receive any

PROPERTY OF NATIONAL PRIVACY COMMISSION

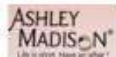


Cyber-Safe

# Uber paid hackers \$100,000 after they stole data on 57 million users **UBER**

by Selena Larson @selenalarson

## Ashley Madison let off with \$1.66m fine over huge hack



## CVS Pays \$2.25 Million in Record HIPAA Settlement



Posted on February 20, 2009

## Home Depot breach totals: 56 million credit cards exposed, \$62 million in losses



## Yahoo Says 1 Billion User Accounts Were Hacked

By VINU GDEI and NICOLE PERI ROTH DEC. 14, 2016



## 55M at risk in 'Comeleak'

By Yina G. Santos - Reporter | @santustina19Q Philippine Daily Inquirer 7:12:44 AM April 21, 2016

## Target Data Breach Has Cost Banks \$240M So Far



## Will Walgreens' \$1.44M HIPAA Privacy Breach Case Set Legal Precedent?



## BOEING NOTIFIES 36,000 EMPLOYEES FOLLOWING BREACH

by Chris Brook



February 27, 2017, 3:48 pm





# No Business Wants a Data Breach

Impact of data breaches  
on businesses:



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

# RESILIENCE & THE FILIPINO SPIRIT

DP

NON-BANK FINANCIAL INSTITUTIONS



15

COMMISSION





# RESILIENCE & THE FILIPINO SPIRIT



15

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 & THE FILIPINO SPIRIT

D P

NON-BANK FINANCIAL INSTITUTIONS



15

SSION





# Resilience



## Resilience

- rɪˈzɪliəns/

- *noun*

- 1. the **capacity to recover quickly from difficulties;** toughness.

- adapt well to change

- keep going in the face of adversity

# 21<sup>st</sup> Century Hazards and Risks

DP 15

NON-BANK FINANCIAL INSTITUTIONS



DATA PRIVACY COMMISSION



## Norse – Superior Attack Intelligence

Norse monitors the world's largest distributed denial-of-service (DDoS) attack network. With over eight million sensors that include over six thousand appliances – 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 Alerts the data through the Norse Applet, which pro-actively finds attacks and improves your overall security. NORSE, and the Norse Intelligence Service, which provides professional real-time threat monitoring for high networks.



LIVE ATTACKS						
TIMESTAMP	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT	
20:41:52.883	134.56.20.778	Philippine Long Distance Telephone Company	Panaytag, PH	Lyranwood, US	23	
20:41:52.498						
20:41:52.661		Philippine Long Distance Telephone Company	207.46.100.251 Redmond, US	De Kalb Junctio... smtp	25	
20:41:51.778	13.0541.357	Philippine Long Distance Telephone Company	122.54.183.239 Manila, PH	Doha, AE	23	
20:41:51.592						
20:41:51.417		Philippine Long Distance Telephone Company	65.55.169.250 Washington, US	De Kalb Junctio... smtp	25	
20:41:51.053	134.56.20.333	Philippine Long Distance Telephone Company	122.3.47.120 Panaytag, PH	Lyranwood, US	23	
20:41:50.732						
20:41:50.604			182.180.160.97 Lahore, PK	Aix-En-Provenc... netis-router	53	

PROPER



# The Data Privacy Act of 2012

---

A 21st Century **Law**

**For 21st Century  
concerns...**



 NORSE





# What is a Privacy Risk?

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







## **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.**



# Disaster



PROPERTY OF NATIONAL PRIVACY COMMISSION



# Resilience





THE PRIVACY COMMISSIONER

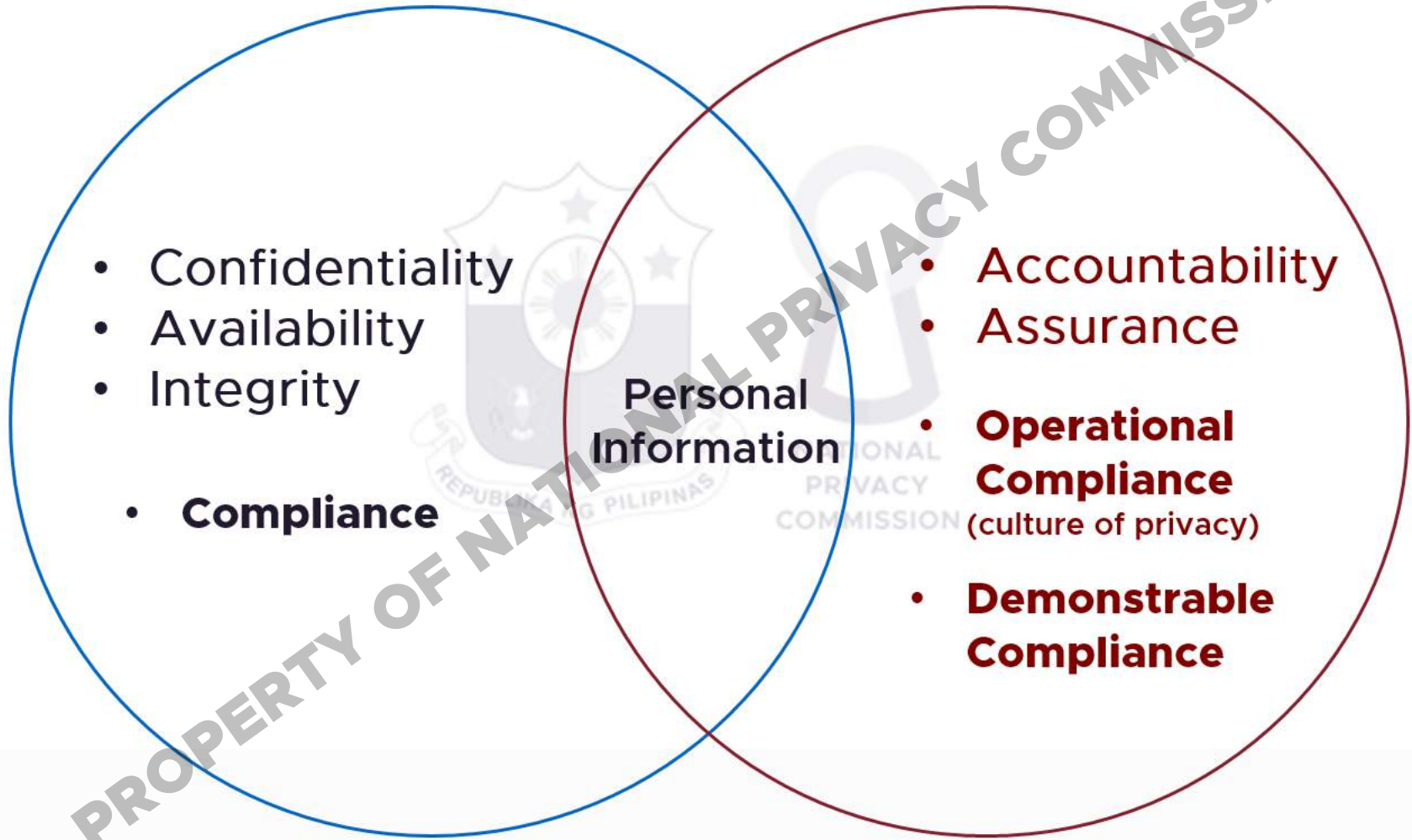
# Philosophy

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

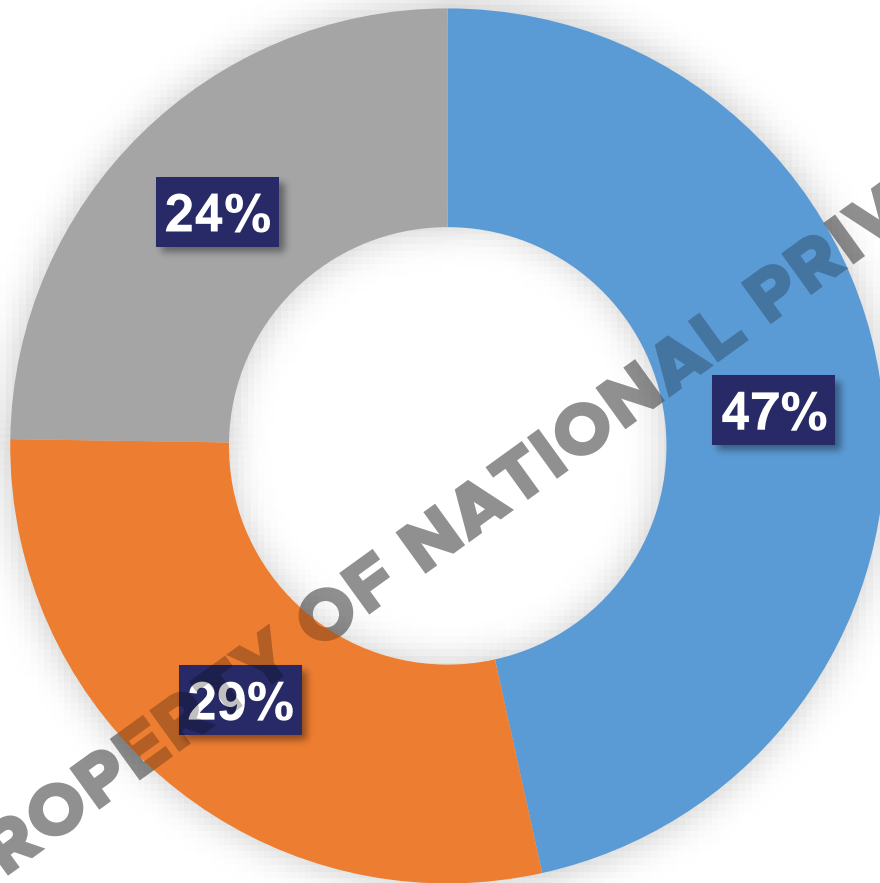


# Data Protection

# Data Privacy



# ROOT CAUSES OF BREACH



- **Malicious or criminal attack**
- **System Glitch**
- **Human Error**



# HOW DO PRIVACY BREACHES OCCUR?

- **lost or stolen laptops**, removable storage devices, or paper records containing personal information
- **hard disk drives and other digital storage** media (integrated in other devices, for example, multifunction printers, or otherwise) 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

# HOW DO PRIVACY BREACHES OCCUR?

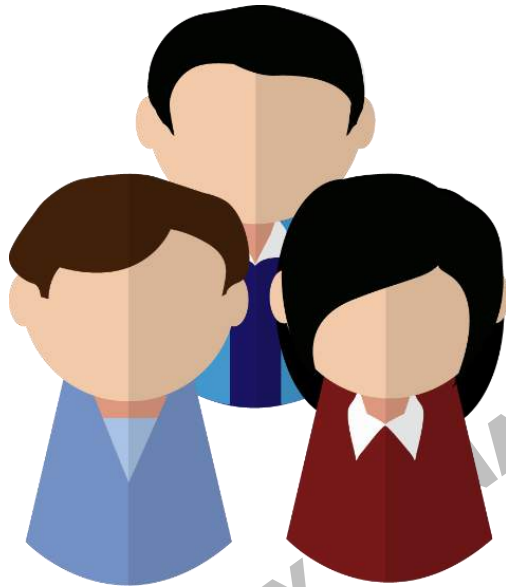
- **employees accessing** or disclosing personal information outside the requirements or authorization of their employment
- **paper records stolen** from insecure recycling or garbage bins
- an agency or organization **mistakenly providing personal information** to the wrong person, for example by sending details out to the wrong address, and
- an **individual deceiving an agency** or organization into improperly releasing the personal information of another person.

# DATA PRIVACY RELATED DIFFICULTIES

DP  
NON-BANK FINANCIAL INSTITUTIONS



15



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

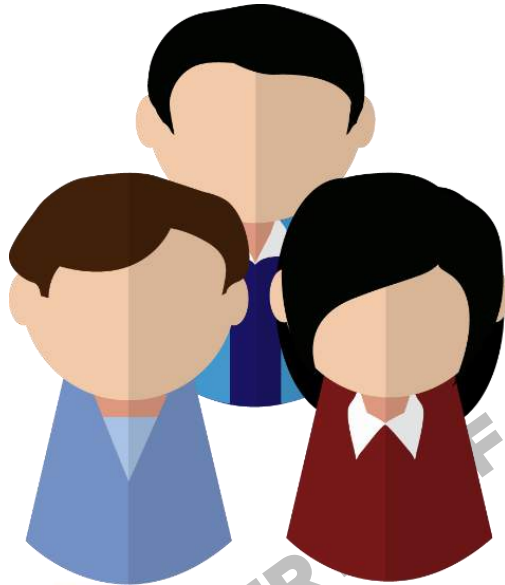


# PROCESSING PERSONAL INFORMATION CAN CREATE PROBLEMS FOR INDIVIDUALS

**DP**  
NON-BANK FINANCIAL INSTITUTIONS



**15**



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

# STRUCTURE OF RA 10173

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

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

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

**Sections 25-37.**  
Penalties  
.....

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





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,  
Commission,  
and for other purposes



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

NULL 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**





THE SCOPE AND POLICY OF



THE DATA PRIVACY ACT OF 2012

# The Privacy Ecosystem

YOU  
The Data  
Subject



REGULATORS  
The NPC

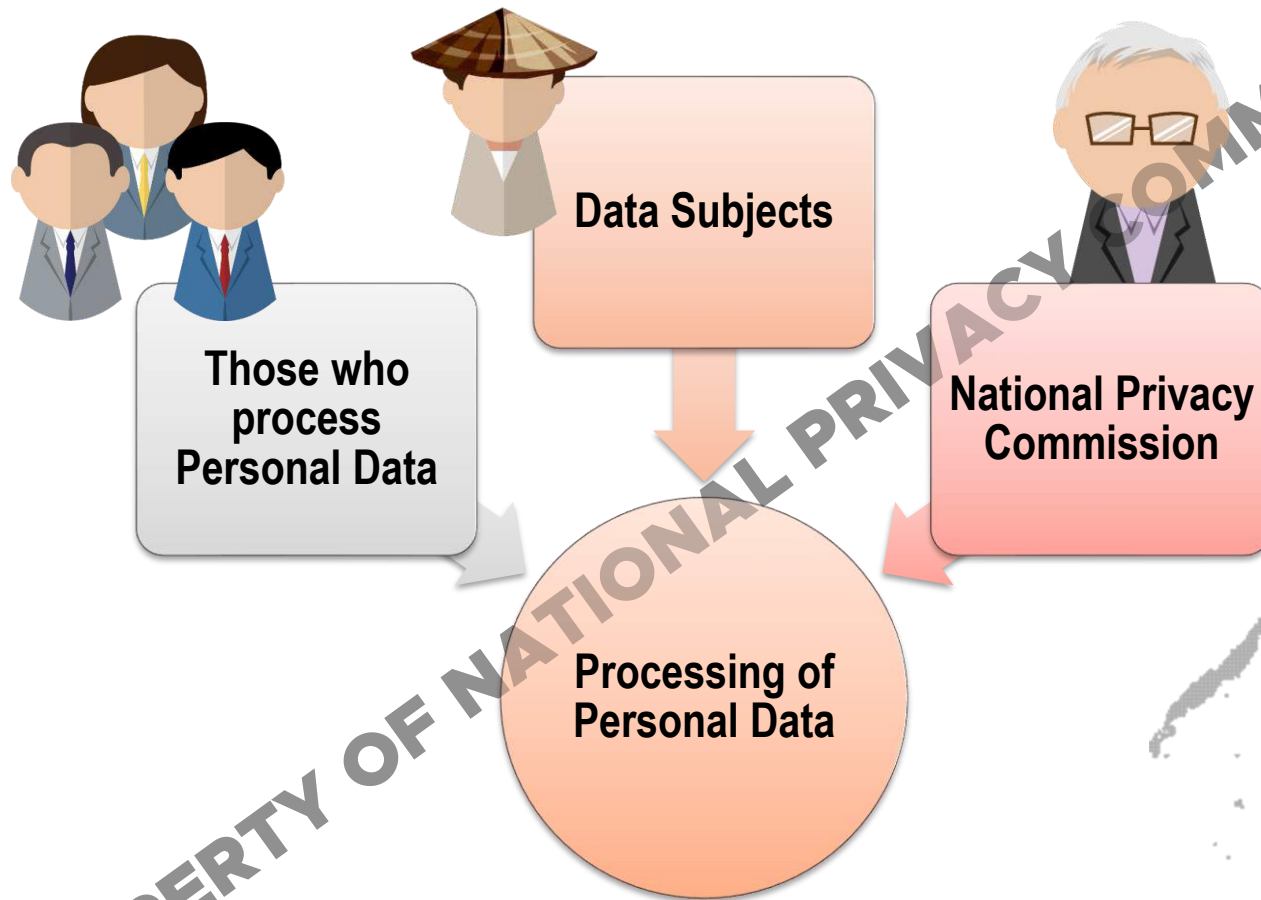
ORGANIZATIONS  
Personal Information  
Controllers & Processors



# 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 NATIONAL PRIVACY COMMISSION





# PERSONAL INFORMATION CONTROLLER

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.

It excludes:

- ✂ A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
- ✂ A natural person who processes personal data in connection with his or her personal, family, or household affairs;



# PERSONAL INFORMATION PROCESSOR



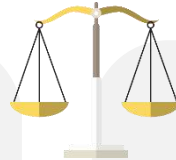
Refers to any natural or juridical person or any other body to whom a personal information controller may **outsource or instruct the processing of personal data** pertaining to a data subject.

PROPERTY OF 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.

PROPERTY OF NATIONAL PRIVACY COMMISSION

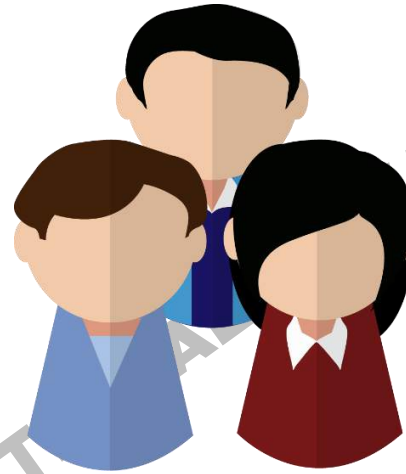


# DATA SUBJECT

DP  
NON-BANK FINANCIAL INSTITUTIONS



15



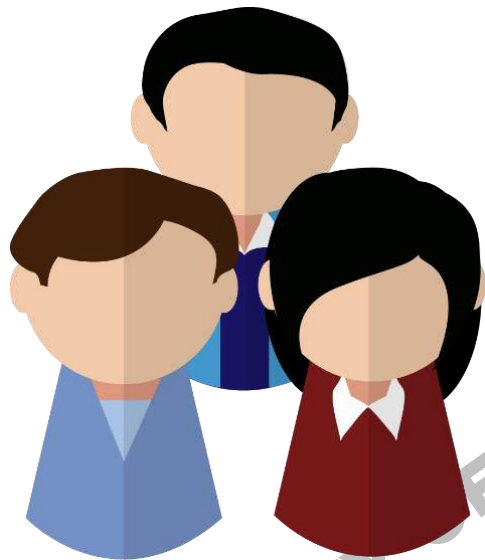
An individual whose **personal, sensitive personal or privileged information is processed.**

# RIGHTS OF A DATA SUBJECT

DP  
NON-BANK FINANCIAL INSTITUTIONS



15



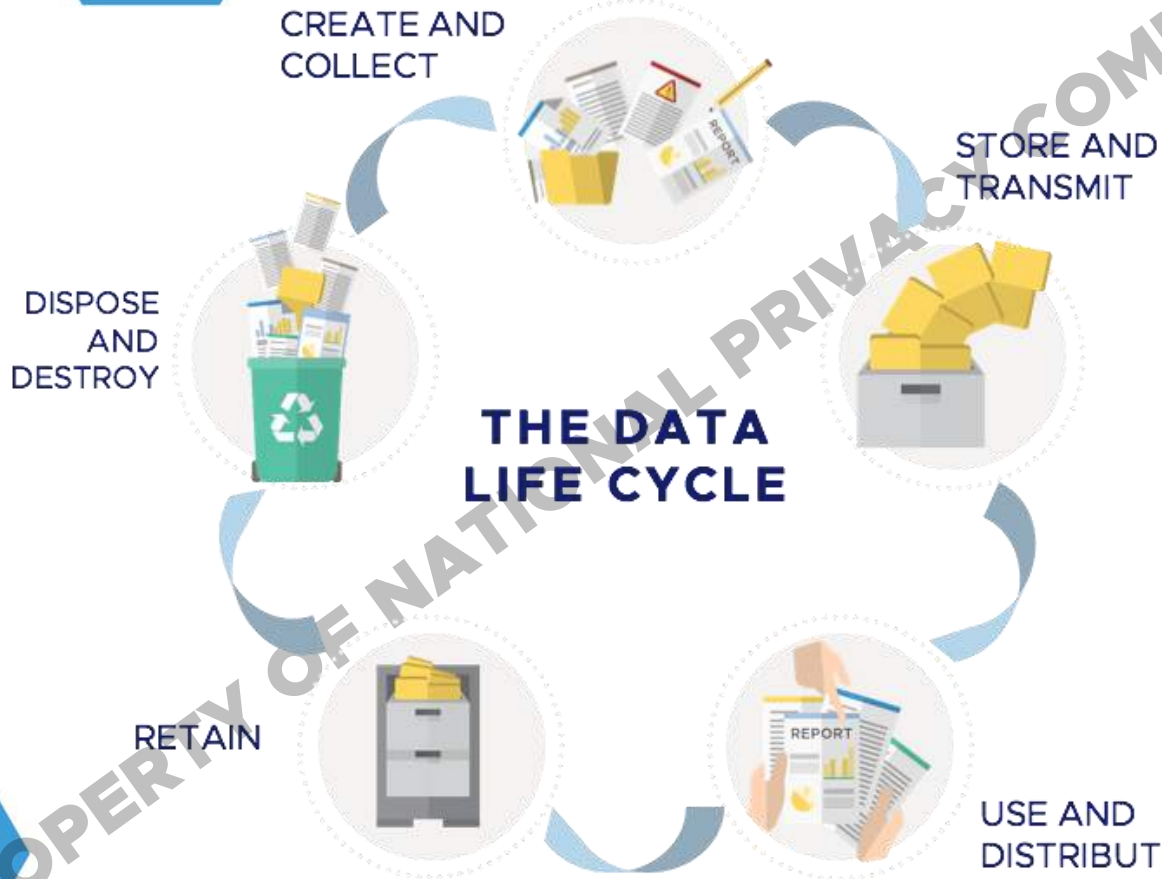
1. Right to be Informed
2. Right to Access
3. Right to Object
4. Right to Rectification
5. Right to Erasure or Blocking
6. Right to Damages
7. Right to Data Portability
8. Right to File A Complaint

**DP**



**15**

NON-BANK FINANCIAL INSTITUTIONS





# I. CREATE AND COLLECT

**DP**

NON-BANK FINANCIAL INSTITUTIONS



**15**



<b>Punishable Act</b>	<b>Imprisonment</b>	<b>Fine (PHP)</b>
Unauthorized Purposes	18 months to 5 years – 2 years to 7 years	500 thousand to 2 million
Unauthorized Processing of Personal Information/Records	1 year to 3 years – 3 years to 6 years	500 thousand to 4 million

## II. STORE AND TRANSMIT



**DP**  **15**  
NON-BANK FINANCIAL INSTITUTIONS



<b>Punishable Act</b>	<b>Imprisonment</b>	<b>Fine (PHP)</b>
Accessing of Personal Information and Sensitive Personal Information due to Negligence	1 year to 3 years – 3 years to 6 years	500 thousand to 4 million
Intentional Breach	1 year to 3 years	500 thousand to 2 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years – 3 years to 5 years	500 thousand to 2 million

# III. USE AND DISTRIBUTE



<b>Punishable Act</b>	<b>Imprisonment</b>	<b>Fine (PHP)</b>
Unauthorized Processing of Personal Information and Sensitive Personal Information	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Unauthorized Purposes	18 months to 5 years — 2 years to 7 years	500 thousand to 2 million
Intentional Breach	1 year to 3 years	500 thousand to 2 million
Concealing Breach	18 months to 5 years	500 thousand to 1 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 2 million



# IV. RETAIN



<b>Punishable Act</b>	<b>Imprisonment</b>	<b>Fine (PHP)</b>
Access due to Negligence of Records	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 1 million

# V. DISPOSE AND DESTROY

**DP**  **15**  
NON-BANK FINANCIAL INSTITUTIONS



<b>Punishable Act</b>	<b>Imprisonment</b>	<b>Fine (PHP)</b>
Improper Disposal of Records	6 months 2 years — 1 year to 3 years	100 thousand to 1 million
Access due to Negligence	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Concealing Breach	18 months to 5 years	500 thousand to 1 million

# DATA PRIVACY PRINCIPLES

---



**TRANSPARENCY**



**LEGITIMATE  
PURPOSE**



**PROPORTIONALITY**



# TRANSPARENCY

DP



15

NON-BANK FINANCIAL INSTITUTIONS



## 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.**

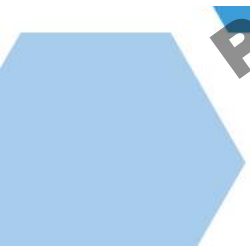


# *Consent of the data subject*



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.

PROPERTY OF NATIONAL PRIVACY COMMISSION



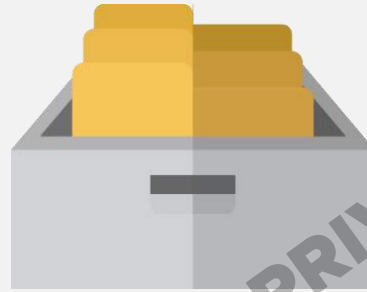
# LEGITIMATE PURPOSE



**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. 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
- GO-MAKER
- X-RAY (WHOLE BODY)
- POLICE CLEARANCE
- PROOF OF BILLING
- FORM 137

# Rule XI. Registration and Compliance Requirements



## Section 46. **Enforcement of the Data Privacy Act.**

Pursuant to the mandate... to administer and implement the Act, and to ensure the compliance... the Commission requires the following:

- a. Registration of personal data processing systems... of at least one thousand (1,000) individuals...**
- b. Notification of automated processing operations... that would significantly affect the data subject;**
- c. Annual Report of the summary of security incidents...**



- d. Compliance with other requirements that may be provided in other issuances of the Commission**



THE FIVE

Pillars

OF

Compliance



# The NPC's 5 Pillars of Accountability and Compliance





## INSTRUCTIONS:

Take a blank sheet of paper and number it from **1 to 20**. For each item, write **T** if true, **F** for false, and **D** if you do not know.



1 \_\_\_\_\_  
2 \_\_\_\_\_  
3 \_\_\_\_\_

We process personal information of Filipino citizens.

We process personal information of citizens from other countries.

The total number of data subjects whose records we store is more than 250.

The total no. of data subjects whose records we store is more than 100,000.

PROPERTY OF NATIONAL PRIVACY COMMISSION



The total number of employees in our organization is more than 1,000.

We process personal information that is classified as "sensitive" by RA 10173.

We issue unique identification numbers or documents such as passport, license, membership card.

We process personal information on paper and other analog media such as microfilm or microfiche.

PROPERTY OF NATIONAL PRIVACY COMMISSION

We process personal information on digital media such as hard disks or servers.

The personal information that we process is scattered over several sites.

We store personal information in the cloud.

We have contracts with service providers to store or process personal information.

PROPERTY OF NATIONAL PRIVACY COMMISSION

As of today, our organization has no privacy or data protection policies.

The personal information we keep is accessed by other companies/agencies.

The personal information we keep is accessed from other parts of the world.

The personal information we keep must be accessible 24 hours a day, 7 days a week.

PROPERTY OF NATIONAL PRIVACY COMMISSION

There is a sub-second response time requirement for access to the personal information we keep.

The number of people who have access to the personal information we keep is more than 50.

The number of people who have access to the personal information we keep is more than 250.

We have ongoing projects where we use personal information in big data or data analytics.

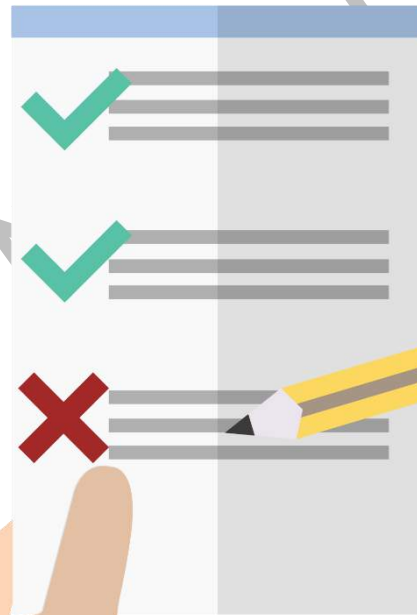
PROPERTY OF NATIONAL PRIVACY COMMISSION



D P  15

LET US SCORE!

You get **five (5)** points for every T  
You get **five (5)** points for every D



PRIVACY COMMISSION

PROPERTY OF

D P

BANK FINANCIAL INSTITUTIONS



15

71+

41-70

0-40

How did you score?



PRIVACY RISK	BENEFIT	CONTROLS	IMPACT ASSESSMENT
High	Low		Unacceptable
Medium	Medium	High	Unreasonable
Low	High	Low	Acceptable
Medium	Medium	Medium	Acceptable

Privacy risk is the probability that the data processing or other activity involving data will result in a loss of the rights and freedoms of an individual.

# THE NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK



A. Choose a DPO



B. Register  
C. Records of processing activities  
D. Conduct PIA



E. Privacy Management Program  
F. Privacy Manual



G. Privacy Notice  
H-O. Data Subject Rights  
P. Data Life Cycle



Q. Organizational  
R. Physical  
S. Technical  
▶ Data Center  
▶ Encryption  
▶ Access Control Policy



T. Data Breach Management;  
▶ Security Policy  
▶ Data Breach Response Team  
▶ Incident Response Procedure  
▶ Document  
▶ Breach Notification



U. Third Parties;  
▶ Legal Basis for Disclosure  
▶ Data Sharing Agreements  
▶ Cross Border Transfer Agreement



V. Trainings and Certifications  
W. Security Clearance



X. Continuing Assessment and Development  
▶ Regular PIA  
▶ Review Contracts  
▶ Internal Assessments  
▶ Review PMP  
▶ Accreditations



Y. New technologies and standards  
Z. New legal requirements



I. Establishing Data Privacy Governance

1. Appointment of your Data Privacy Officer (DPO)

II. Risk Assessment

2. Register

3. Records of processing activities

4. Conduct of a Privacy Impact Assessment (PIA)

III. Preparing Your Organization's Data Privacy Rules

5. Formulate your organization's privacy management program (PMP)

6. Craft your agency's privacy manual

IV. Privacy in Day-to-Day Information Life Cycle Operations (To Be Included in the Privacy Manual)

7. Informing data subjects of your personal information processing activities and obtain their consent, when necessary. (Privacy Notice)

8. Formulation of policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them

9. Policies for limiting data processing according to its declared, specified and legitimate purpose

10. Policies/procedures for providing data subjects with access to their personal information including its sources, recipients, method of collection, purpose of disclosure to third parties, automated processes, date of last access, and identity of the controller (Data Subject Access Request)

11. Policies/procedures that allow data subjects to dispute inaccuracy or error of their personal information including policies/procedures to keep the same up to date

12. Policies/procedures that allow a data subject to suspend/withdraw or order the blocking, removal or destruction of their personal information

CREATION AND COLLECTION,  
STORAGE, TRANSMISSION, USE AND DISTRIBUTION,  
RETENTION, AND  
DESTRUCTION/  
DISPOSAL

# THE NPC'S 32-PT. DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE CHECKLIST

20. Compliance with the DPA's Data Breach Management Requirements (e.g. Security Policy, Data Breach Response Team, Incident Response Procedure, Document, Breach Notification)

VII. Managing Third Party Risks

21. Maintaining data privacy requirements (Legal Basis for Disclosure, Data Sharing Agreements, Cross Border, Security of Transfers) for third parties (e.g. clients, vendors, processors, affiliates)

VIII. Managing Human Resources (HR)

22. Periodic and mandatory personnel training on privacy and data protection in general and in areas reflecting job-specific content

23. Issuance of Security Clearance for those handling personal data

IX. Continuing Assessment and Development

24. Scheduling of Regular PIA for new and existing programs, systems, processes and projects

25. Review of Forms, Contracts, Policies and Procedures on a regular basis

26. Scheduling of Regular Compliance Monitoring, Internal Assessments and Security Audits

27. Review, validation and update of Privacy Manual

28. Regular evaluation of Privacy Management Program

29. Establishing a culture of privacy by obtaining certifications or accreditations vis-à-vis existing international standards

X. Managing Privacy Ecosystem

30. Monitoring of emerging technologies, new risks of data processing, and the Privacy Ecosystem

31. Keeping track of data privacy best practices, sector specific standards, and international data protection standards

32. Seeking guidance and legal opinion on new National Privacy Commission (NPC) issuances or requirements

## AREA I. Establishing Data Privacy Governance

**Item #1. Appoint Data Protection Officer**

## AREA II. Risk Assessment

**Item #2. Register**

**Item #3. Records of Processing Activities**

**Item #4. Conduct of a Privacy Impact Assessment (PIA)**

## AREA III. Preparing Your Organization's Data Privacy Rules

**Item #5. Formulate your organization's privacy management program (PMP)**

**Item #6. Develop your agency's privacy manual and complaints mechanism**



## AREA IV: Privacy in Day-to-Day Information Life Cycle Operation

Item #7. Informing data subjects of your personal processing activities and obtain their consent, when necessary.

Item #8. Formulation of policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them.

Item #9. Policies for limiting data processing according to its declared, specified and legitimate purpose.

Item #10. Policies/ procedure providing data subjects with access to their personal information including its sources, recipient, method of collection, purpose of disclosure to third parties, automated processes, date of last access, and identity of controller

Item #11. Policies/procedure that allow data subjects to dispute accuracy or error of their personal information including policies/procedure to keep the same up to date.

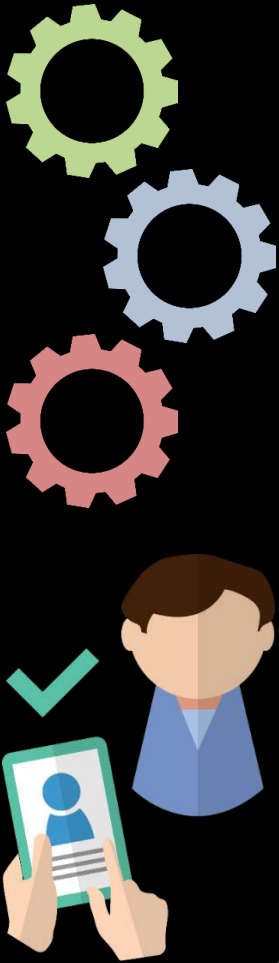
Item #12. Policies/ procedure that allow data subjects to suspend, withdraw or order the blocking, removal or destruction of their personal information.

Item #13. Policies/procedure for accepting and addressing complaints from data subjects.

Item #14. Policies/procedures that allow data subjects to get indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false and unlawfully obtained or unauthorized use of personal information.

Item #15. Policies/procedures that allow data subjects to obtain from the personal information controller a copy of his or her personal data processed by electronic means and in a structured and commonly used format.

Item #16. Policies/procedures for creation and collection, storage, transmission, use and distribution, retaining personal data for only a limited period or until the purpose of the processing has been achieved, and ensuring that data is securely destroyed or disposed of



### AREA V. Managing Personal Data Security Risk

Item #17. Implement appropriate and sufficient organizational security measures

Item #18. Implement appropriate and sufficient physical security measures

Item #19. Implement appropriate and sufficient technical security measures

### AREA VI. Data Breach Management

Item #20. Compliance with the DPA's Data Breach Management Requirements

### AREA VII: Managing Third Party Risk

Item #21: Maintaining data privacy requirements for third parties (e.g. clients, vendor, processor, affiliates)? (Compliance, Agreement, Due Diligence, Notifications, Access Policies.)

### AREA VIII. Managing Human Resources (HR)

Item #22. Periodic and mandatory personnel training on privacy and data protection in general and in areas reflecting job-specific content

Item #23. Issuance of Security Clearance for those handling personal data

### AREA IX. Continuing Assessment and Development

Item #24. Scheduling of Regular PIA for new and existing programs, systems, processes and projects

Item #25. Review of Forms, Contracts, Policies and Procedures on a regular basis

Item #26. Scheduling of Regular Compliance Monitoring, Internal Assessments and Security Audits

Item #27. Review, validation and update of Privacy Manual

Item #28. Regular evaluation of Privacy Management Program

Item #29. Establishing a culture of privacy by obtaining certifications or accreditations vis-à-vis existing international standards

### AREA X. Managing Privacy Ecosystem

Item #30. Monitoring of emerging technologies, new risks of data processing, and the Privacy Ecosystem

Item #31. Keeping track of data privacy best practices, sector specific standards, and international data protection standards

Item #32. Seeking guidance and legal opinion on new National Privacy Commission (NPC) issuances or requirements

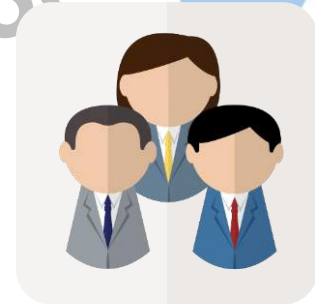






## What do we look for when the NPC comes knocking at your door?

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**?



# Cultivating a Culture of Trust



**Trust is the product of...**

**Value**


**Respect**

**Security**

# Building a regime of Trust





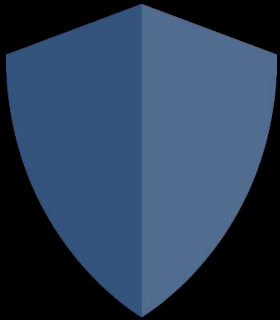


# ***When will you hear from the NPC?***

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**

# The Data Privacy Golden Rule

---



If you Can't Protect It...

**DONT Collect It.**



**Thank you  
for listening!**

*[facebook.com/privacy.gov.ph](https://facebook.com/privacy.gov.ph)  
[twitter.com/privacyPH](https://twitter.com/privacyPH)  
[info@privacy.gov.ph](mailto:info@privacy.gov.ph)*



**Leandro Angelo Y. Aguirre**  
Deputy Privacy Commissioner  
20 February 2018