



# “THE PRIVACY LAW AND IMPACT ON PRIVATE HEALTH CARE PROVIDERS”

Raymund E. Liboro  
Privacy Commissioner  
and Chairman



# 1995





# 2015



# Forbes Most Valuable Brands 2007 Versus 2017



Exxon Mobil



PetroChina



General Electric



China Mobile



ICBC



Microsoft



Royal Dutch



GazProm



AT&T



Apple



Google



Microsoft



Facebook



Coca Cola



Amazon



Disney



Toyota



McDonalds



Samsung



# DATA IS THE NEW OIL

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

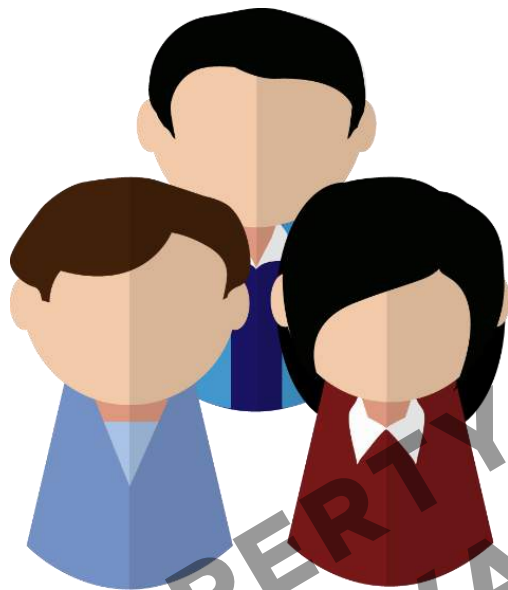


ALIBABA



AIRBNB

# 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





1004



30



2



0



1

# 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 Lontok said he received notifications from three banks saying that he borrowed a

~~Mark Joseph Lontok~~ 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, ~~\_\_\_\_\_~~ remembered posting a photo of his Professional Regulation Commission (PRC) ID online.

"Wala naman akong ginagawang masama," he added.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION



# 55M at risk in 'Comeleak'

By: [Tina G. Santos](#) - Reporter / @santostinaINQ Philippine Daily Inquirer / 12:44 AM April 23, 2016



**DECEPTIVE CALM** The Comelec office at Palacio del Gobernador in Intramuros, Manila, after office hours. The Comelec says the hacking of its website will not compromise the integrity of national elections on May 9.  
EDWIN BACASMAS







news.abs-cbn.com/halalan2016/nation/04/29/16/natl-privacy-commission-probes-comelec-hacking

# Nat'l Privacy Commission probes Comelec hacking

ABS-CBN News

Posted at 29 Apr 2016 04:45 PM

MANILA - The National Privacy Commission has started its investigation into the recent hacking of the Commission on Elections (Comelec) after receiving an **initial report** from the poll body Friday.

Under the Data Privacy Act, the National Privacy Commission has to be notified about the hacking. The body is tasked to monitor government agencies and private organizations handling sensitive data.



PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION



## Identity thieves can:

- Get a Loan
- Open Credit Cards
- Open Utility Accounts
- Apply for a Refund
- Apply for Employment
- Get Medical Care
- Commit Crime or Fraud

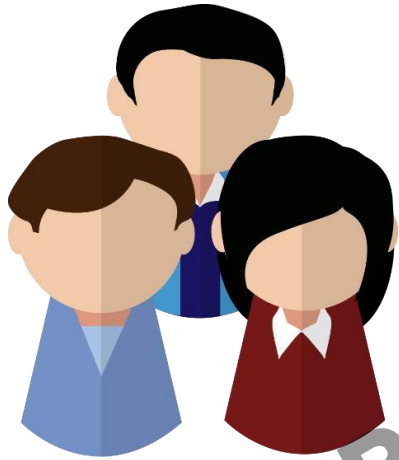
## Impact on victims:

- denial of credit/loans
- denial of public service
- denial of medical care
- harassment by collectors
- lawsuits
- stress/anxiety
- embarrassment
- time/expenses spent on recovery steps





## *Impact of a Problematic Data Action on Business*



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



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:

[See Your Matches »](#)

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

100%  
Like-minded  
People

**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!

COMMISSION

# ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

See your Match

Over 37,55,000 anonymous members!





Ashley Madison

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

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



This article is 3 months old

55 60

Readers in Toronto

Thursday 18 December 2016 12:40 PM



Regulators suspended most of the \$17.5m fine because the company was unable to pay a whopping part of business. Photograph: Reuters/Chris Wedel/Getty Images

The owners 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.

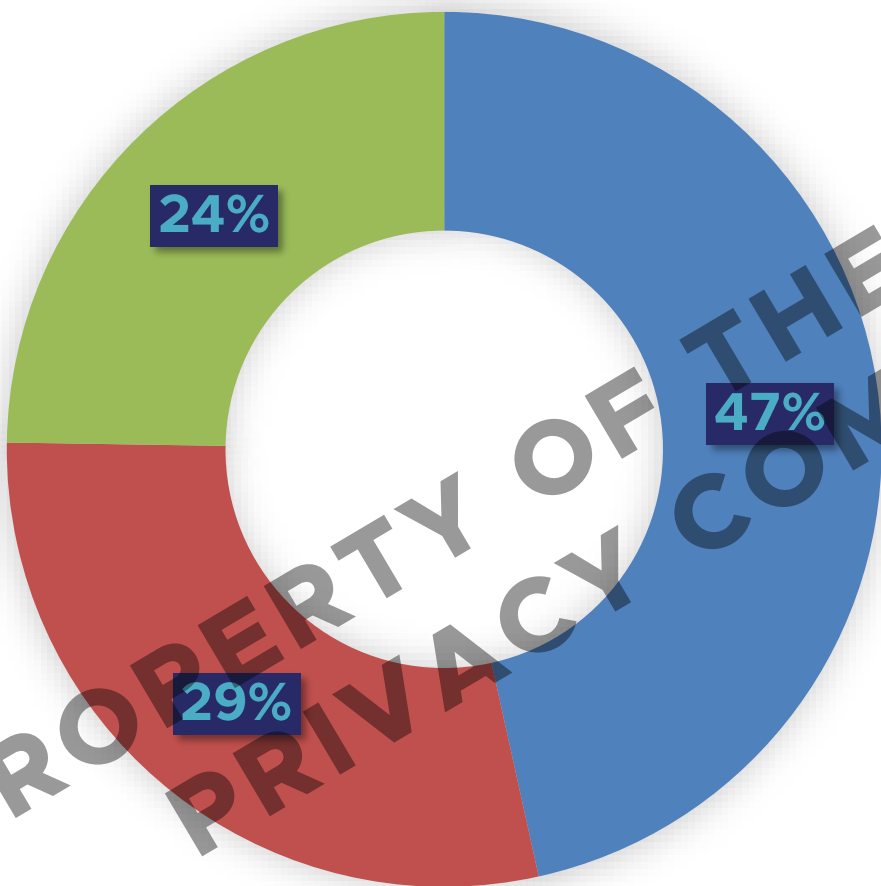
The remainder of a \$17.5m settlement was suspended based on privately held Ruby Corp's inability to pay.

"I recognize 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 THE INTERNATIONAL PRIVACY COMMISSION

# ROOT CAUSES OF BREACH



■ Malicious or criminal attack

■ System Glitch

■ Human Error



## Report: medical data breach found in 90% of industries

By Carol Ko | 07 Jan 2016

Tag: [data breach](#) [data privacy](#) [healthcare](#) [information security](#) [Verizon Enterprise](#)

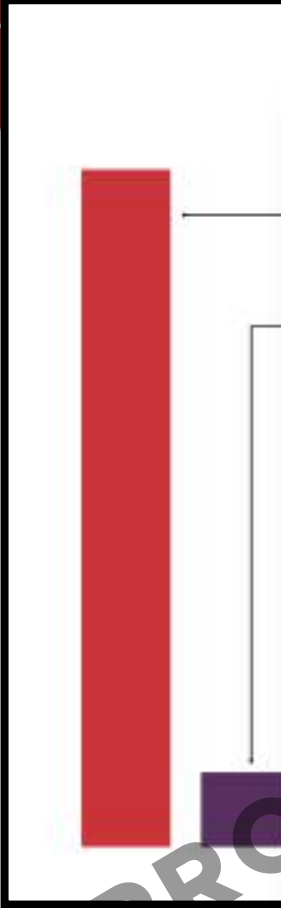


A few years ago, Hong Kong was haunted by a string of data leakage cases involving different public authorities including public hospitals, police, fire services and the

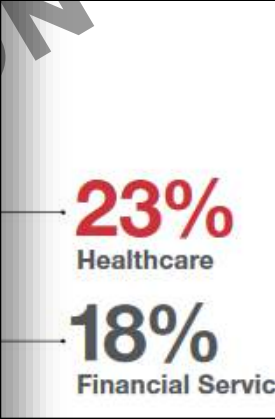
In fact, on a global basis, the healthcare industry was found to be the worst offender of data breaches, among all the industries that involve the handling to personal

“Verizon 2015 Protected Health Information Data Breach Report”

Of all the 392 million records of patient data breaches disclosed worldwide in between 2004 and 2014, 1,403 breaches occurred within the healthcare industry, according to the PHI Data Breach Report. This was far ahead of the next worst offenders: the public sector with 177 data breaches, and the finance industry, with 113 data breaches.



	Frequency Percentage of Incidents by Industry	Severity Average Size of Notification
HEALTHCARE	<i>Healthcare was more frequent but not as severe</i> <b>23%</b>	<b>340K</b>
FINANCIAL SERVICES	<b>18%</b>	<b>2K</b>
EDUCATION	<b>16%</b>	<b>1K</b>
RETAIL	<b>12%</b>	<b>33K</b>
RESTAURANTS/ HOSPITALITY	<b>9%</b>	<i>Restaurants/ Hospitality topped the severity list of number of affected individuals</i> <b>2.2M</b>





# Insiders responsible for 68% of network attacks on healthcare organizations

*Written by Jessica Kim Cohen* | February 24, 2017 | [Print](#) | [Email](#)

There were 320 breaches of unsecured protected health information in 2016, representing an increase of 18.5 percent over 2015, according to an IBM X-Force Research report.



<http://www.beckershospitalreview.com/healthcare-information-technology/insiders-responsible-for-68-of-network-attacks-on-healthcare-organizations.html>

# HOW DO PRIVACY BREACHES OCCUR?

Lost or stolen **Laptops**, removable **storage devices**, or **paper records**

## Healthcare IT News

TOPICS

Privacy & Security

### Unencrypted drive with 7 years of patient data stolen from Denton Heart Group

The backup drive contained a trove of EHR data, including Social Security numbers and insurance policy details.

By Jessica Davis | March 14, 2013 | 11:20 AM



### Stolen laptop may have contained data of 3,600 Children's Hospital of Los Angeles patients

Written by Erin Dietsche (Twitter | Google+) | January 17, 2017 | Print | Email

Children's Hospital Los Angeles began notifying 3,600 patients that their information may have been on a laptop that was stolen from a physician's car, according to the *Los Angeles Times*.

During an Oct. 18 burglary, the laptop was allegedly stolen from a physician's locked car, according to CBS News. It may have contained the names, addresses, medical record numbers and clinical information of patients. Hospital officials said the laptop was protected with a password, but they're unsure whether it was properly encrypted.

Hospital spokesman Lorenzo Benet said CHLA "believe[s] that all data may have been erased from the device without any patient data being accessed," according to the *Los Angeles Times*.



<http://www.beckershospitalreview.com/healthcare-information-technology/kansas-medical-center-breach-affects-6-8k-patients.html>



# HOW DO PRIVACY BREACHES OCCUR?

**Paper records** stolen from insecure **recycling** or **garbage bins**



## Medical billing records found in pile of debris in New Orleans

Written by Erin Dietsche ([Twitter](#) | [Google+](#)) | February 08, 2017 | [Print](#) | [Email](#)

<http://www.beckershospitalreview.com/healthcare-information-technology/medical-billing-records-found-in-pile-of-debris-in-new-orleans.html>

Beatrice August and her husband weren't expecting to find patients' medical billing records in a pile of garbage on their New Orleans property, reports [WDSU](#). But that's exactly what they discovered.

Ms. August said she doesn't know who dumped the debris on the property, which has been in her family for years.

"We came out here in November and we saw the first pile back there," she told [WDSU](#). "Then when we came two weeks later, my husband and I came to check, and we saw this. We said, 'Oh my goodness, this is somebody's personal information out here.'"

Ms. August said she even found a network of insurance records.

"We came out here in November and we saw the first pile back there," she told [WDSU](#). "Then when we came two weeks later, my husband and I came to check, and we saw this. We said, 'Oh my goodness, this is somebody's personal information out here.'"

# HOW DO PRIVACY BREACHES OCCUR?

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

Privacy & Security

**UPDATED: Hospitals in UK National Health Service knocked offline by massive ransomware attack** **MultiCare Health System breach affects 1,200 patients**

Written by [Erin Dietsche](#) (Twitter | Google+) | January 27, 2017 | [Print](#) | [Email](#)

The network was likely taken down by the Wanna Decryptor, one of the most effective ransomware variants for which there's currently no decryptor available.

By [Jessica Davis](#) | May 12, 2017 | 12:56 PM



Tacoma, Wash.-based MultiCare Health System has notified approximately 1,200 current and former patients that their information may have been compromised in a recent privacy incident, according to *The News Tribune*.

In late November, an unauthorized individual may have accessed an employee's email account. Although MultiCare secured the account, an investigation proved the account may have contained sensitive patient information, including names, genders, dates of birth, addresses, dates of service, account balances and diagnosis and treatment information. Patients' Social Security numbers and financial information were not disclosed in the email account.

# HOW DO PRIVACY BREACHES OCCUR?

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



## Virginia Mason Memorial employees illegally access patient health records

Virginia Mason Memorial Hospital recently discovered 21 hospital employees inappropriately accessed patient health records from around October 2016 to January of this year.

According to an article in the [Yakima Herald](#), employees improperly accessed the health information of 419 emergency room patients over a period of about three months.

[READ MORE: 55K Potentially Affected by Virus Encrypting Pediatric Servers](#)

<https://healthsecurity.com/news/kentucky-health-center-ensures-phi-security-after-email-gaffe>

<http://www.beckershospitalreview.com/health-care-information-technology/3-promedica-employees-fired-for-insider-breach-of-nearly-3-500-patients-data.html>

## 3 ProMedica employees fired for insider breach of nearly 3,500 patients' data

Written by Akanksha Jayaraj (Twitter | Google+) | June 06, 2016 | Print | Email

ProMedica has terminated three employees for accessing patient records at two hospitals for reasons unrelated to their job responsibilities, reports *The Toledo Blade*.

In total, seven employees accessed 3,472 patients' medical records at ProMedica's Bixby Hospital in Adrian, Mich., and Herrick Hospital in Tecumseh, Mich. The three employees who were terminated had no reason to access the records, and the other four had authority to access the records under certain circumstances. The four with access are receiving "extensive disciplinary actions," Julie Yaroch, DO, president of Bixby and Herrick hospitals, told *The Toledo Blade*.

The employees accessed patient names, birth dates, medications and clinical information from acute care services. Dr. Yaroch indicated none of the records were printed, and there is no reason to believe the information was recorded for outside use, according to the report.

Another employee of the Toledo, Ohio-based health system alerted hospital administrators of the breach in April, and ProMedica launched an investigation into the incident. Dr. Yaroch informed *The Toledo Blade* of the breach on Friday.







# Information Security

*versus*

# Data Privacy

PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION





## SECURITY

A **Breach** is the unauthorized acquisition, access, use, or disclosure of protected information, which compromises the security or privacy of such information



## PRIVACY

A **Personal data breach** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed

*Personal Information*



## SECURITY

### Impact on Data

- ❖ Confidentiality
- ❖ Integrity
- ❖ Availability

*Governance of the unauthorized*



## PRIVACY

### Impact on people

- ❖ Collection
- ❖ Use
- ❖ Storage
- ❖ Sharing
- ❖ Disposal

*Governance of the authorized*

*Personal Information*

*Sensitive Personal Information*

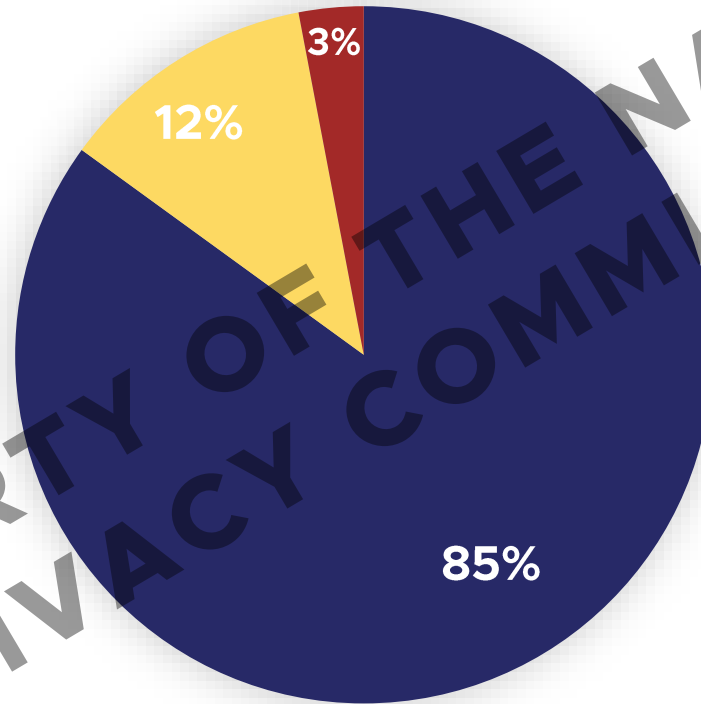




# Survey Results

Importance of The Rights of A Data Subject,  
Philippines, Jun 2017

% of  
Adults



**Net\***  
**+83**

■ Important   ■ Undecided   ■ Not Important

*\*Net figure % Likes to know minus % Does Not like to Know, correctly rounded*

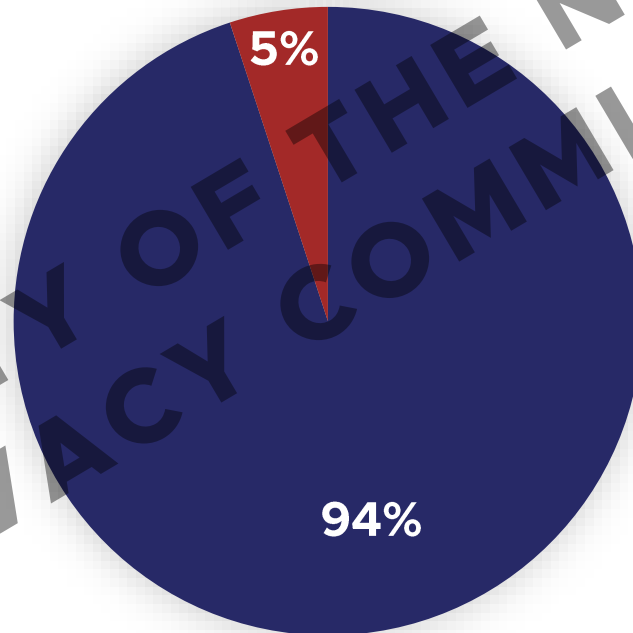
*\*Based on the SWS Survey "FILIPINO PUBLIC OPINION ON DATA PRIVACY AND ATTITUDES AND BEHAVIOUR TOWARDS INTERNET USAGE" June 17-21, 2017 National Survey*



# Survey Results

Extent of Liking or Not Liking to Know Where The Personal Information They Have Provided During Transaction or Application Will Be Used, Philippines, Jun 2017

% of Adults



**Net\***  
**+89**

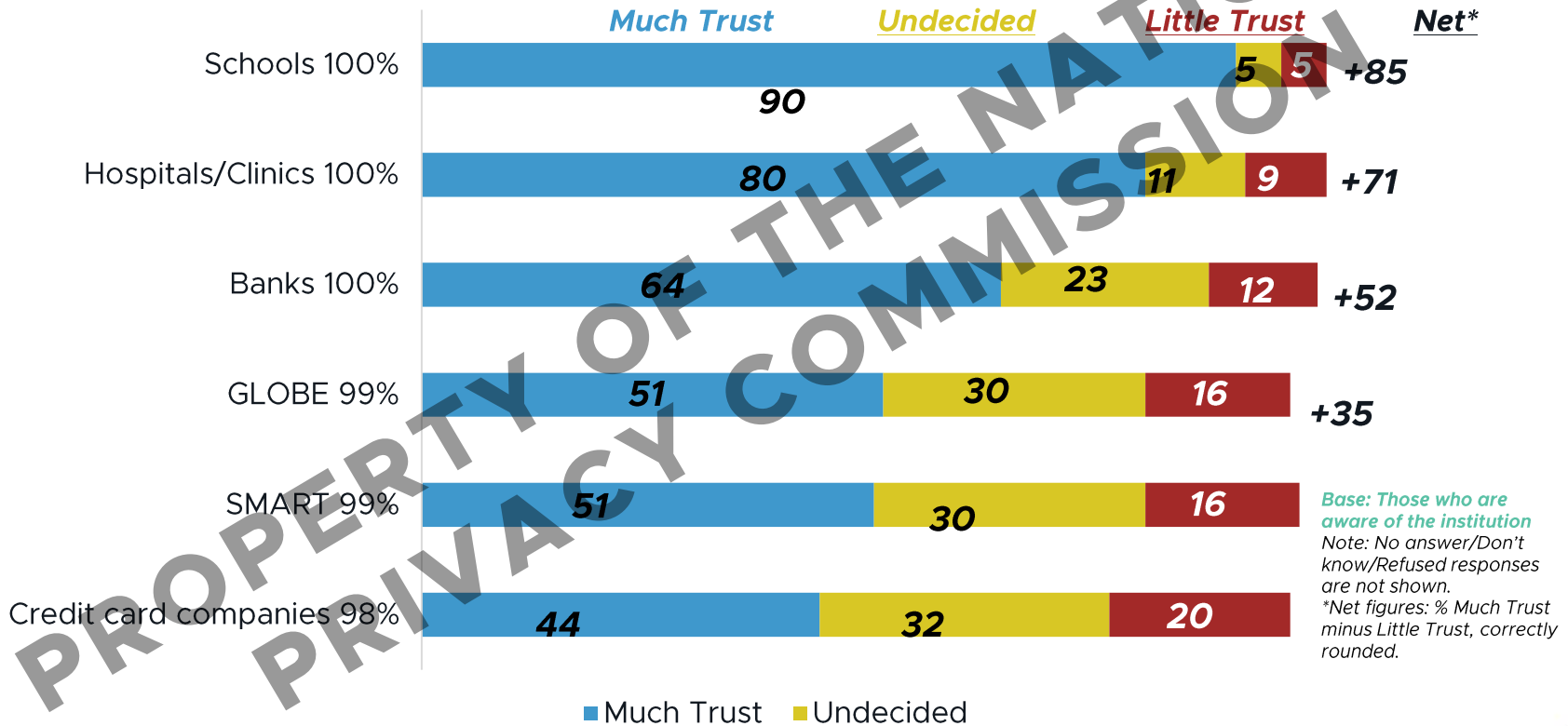
Note: No answer/Don't know/Refused responses are not shown.

\*Net figure % Likes to know minus % Does Not like to Know, correctly rounded

■ Likes to Know ■ Does Not Like to Know

# Survey Results

## Trust in Private Institutions Holding Personal Information, Philippines, Jun 2017





**Browsing History**

**Diary**

**Credit Card Billing Statement**

**Which of the following will you share with a stranger?**

**Home Address**

**Phone Messages**

**Facebook Password**



**NATIONAL  
PRIVACY  
COMMISSION**

PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION



# *The Data Privacy Act (“DPA”) of 2012*

Data privacy - acknowledging the rights of Data Subjects over their data and enforcing the responsibilities of entities who process them





# The Privacy Ecosystem

YOU  
The Data  
Subject



REGULATORS  
The NPC

ORGANIZATIONS  
Personal Information  
Controllers & Processors

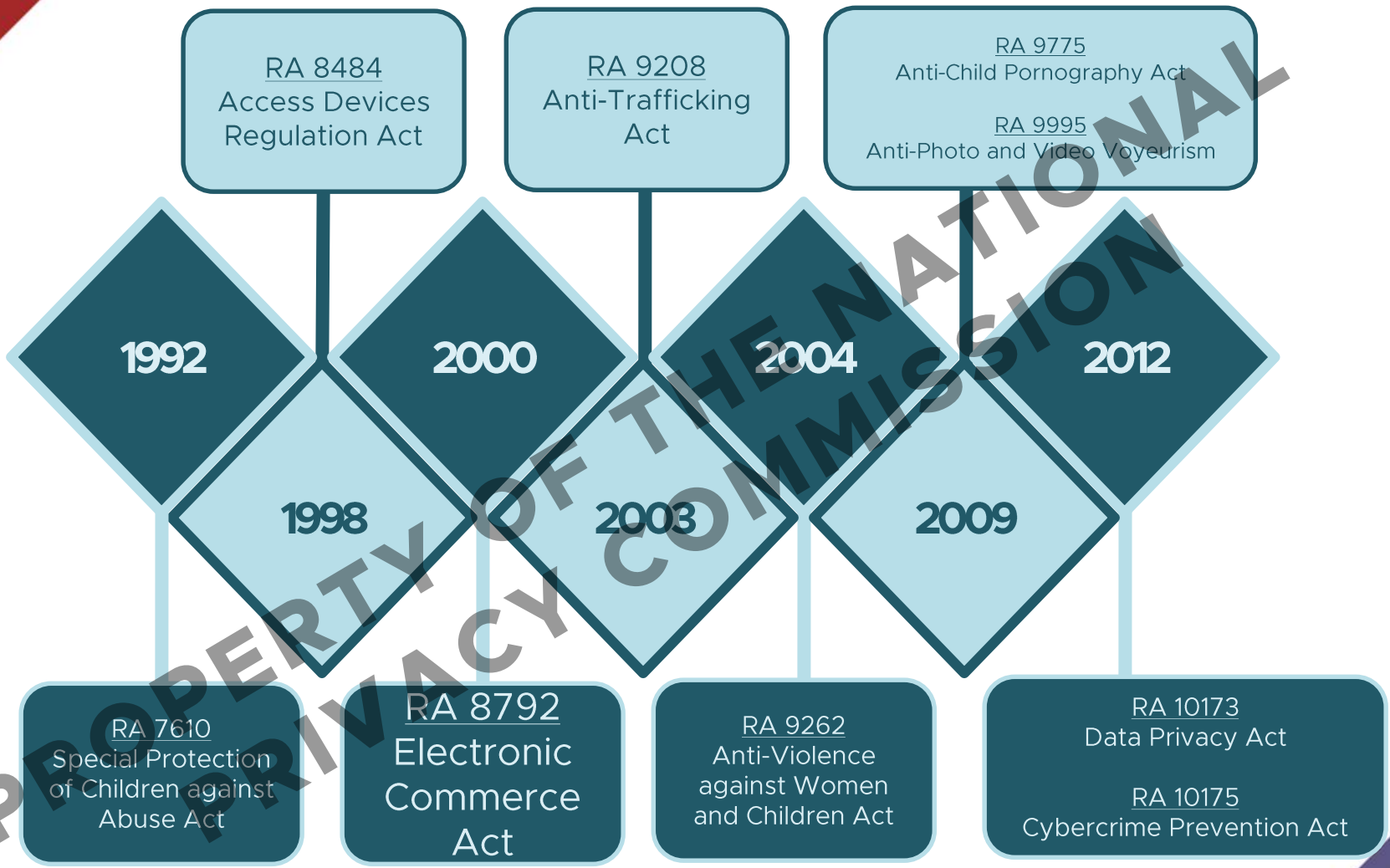
# *Philippine Constitution*

## *Article 3, Bill of Rights*



- **Section 2.** Right to be secure in their persons, houses, papers, and effects against unreasonable searches
- **Section 3.** Privacy of communication and correspondence
- **Section 5.** Free exercise and enjoyment of religious profession and worship
- **Section 6.** Liberty of abode and the right to travel
- **Section 8.** Right to information, and access to official records









THE PRIVACY COMMISSIONER

# Philosophy

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



# Risk Management

- Risk can never be eliminated, so it must be managed.

## Risk Responses

Accept risk  
Avoid risk  
Mitigate risk  
Transfer/share risk



# What is a *Privacy Risk*?

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







AN

*introduction*

TO THE

*Data Privacy Act*

# 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  
.....

## ***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



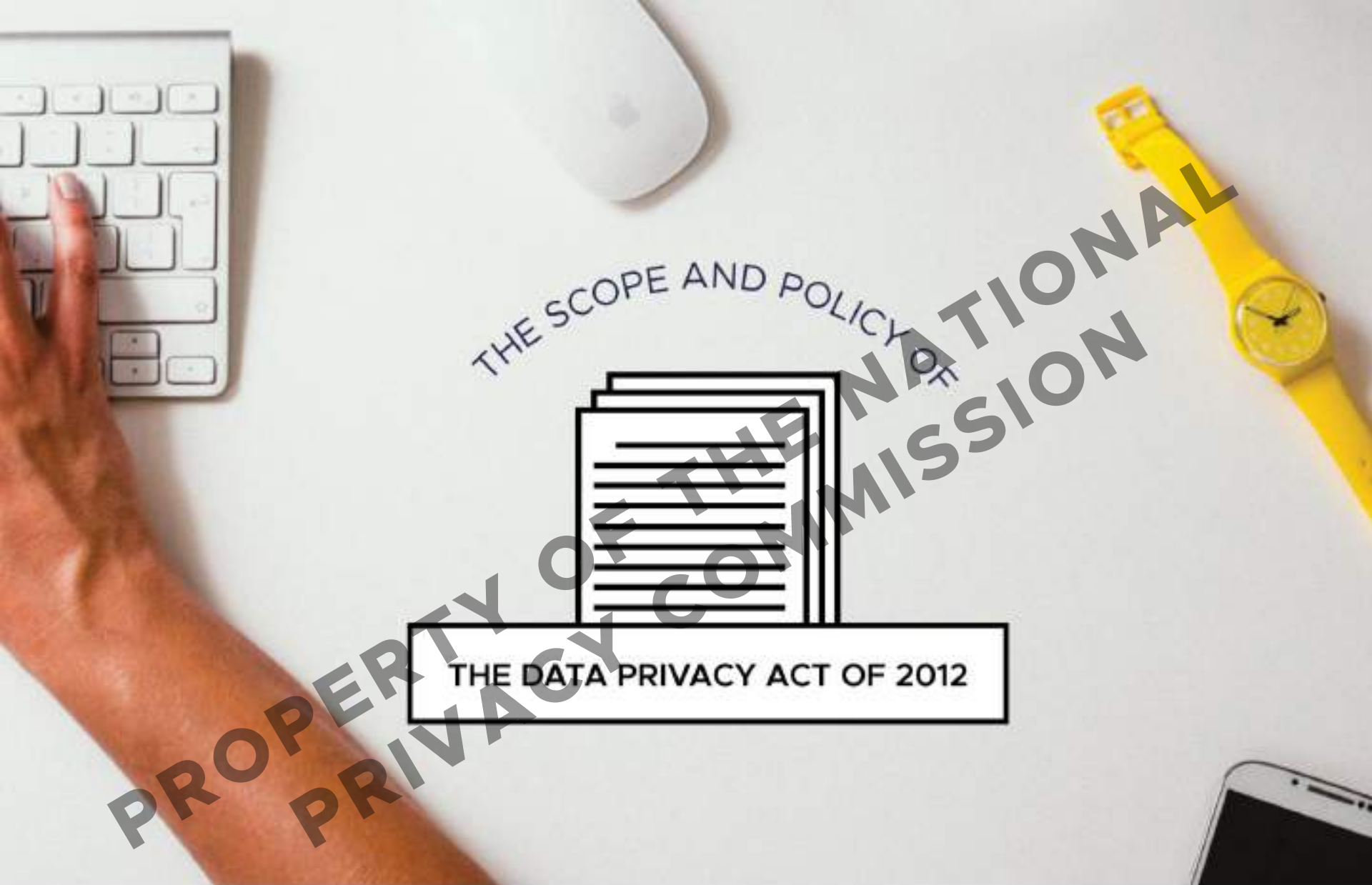


Where  
is **privacy** in  
all of these?

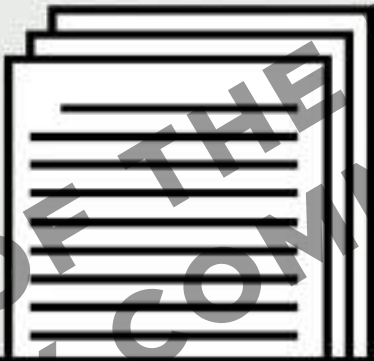
FULL TITLE

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**



THE SCOPE AND POLICY OF



THE DATA PRIVACY ACT OF 2012



THE DATA PRIVACY ACT OF 2012

The rights of a Data Subject



# DATA SUBJECT



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

# RIGHTS OF A DATA SUBJECT



**Right to be Informed**

**Right to Object**



**Right to Access**



PROPERTY OF THE NATIONAL PRIVACY COMMISSION

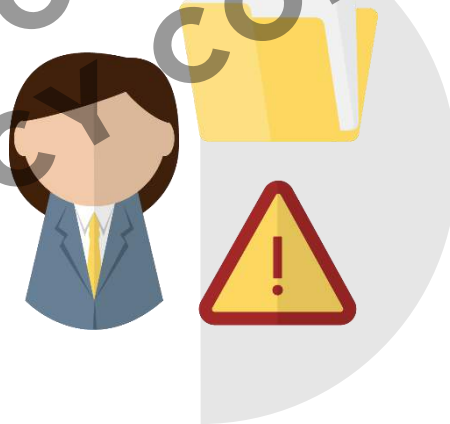


**Right to  
Correct/Rectify**

**Right to  
Block/Remove**



**Right to Data  
Portability**



PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION





**Right to File a Complaint**

**Right to be Indemnified**



PROPERTY OF THE NATIONAL PRIVACY COMMISSION





THE DATA PRIVACY ACT OF 2012

The obligations of data  
controllers and processors

# PERSONAL INFORMATION CONTROLLER



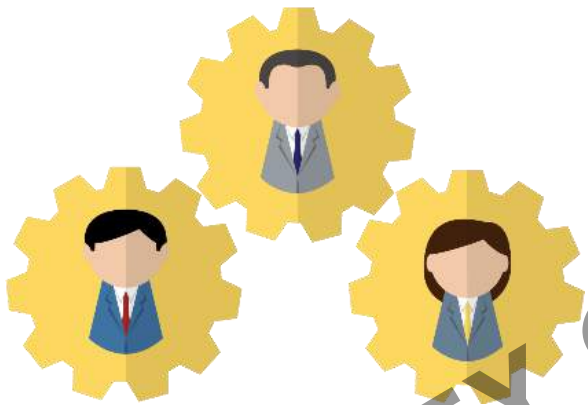
Refers to a natural or juridical person, or any other body who **controls the processing of personal data**, or instructs another to process personal data on its behalf.

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.

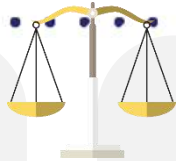
PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION



# 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.



THE DATA PRIVACY ACT OF 2012

The National Privacy  
Commission



# Functions

Advisory

Advocacy

Investigation

Compliance  
& Monitoring

Public  
Education

Complaints

Enforcement

# Rule-Making

# 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.



# 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.

# 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.



CREATE AND  
COLLECT



STORE AND  
TRANSMIT



DISPOSE  
AND  
DESTROY



# THE DATA LIFE CYCLE

RETAIN



USE AND  
DISTRIBUTE



# I. CREATE AND COLLECT



<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



<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

Punishable Act	Imprisonment	Fine (PHP)
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



Punishable Act	Imprisonment	Fine (PHP)
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



<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



# 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.**

# HOW TRANSPARENCY IS DEMONSTRATED

- **CONSENT**
- **PRIVACY NOTICE**
- **PRIVACY POLICY**

PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION







***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 THE NATIONAL  
PRIVACY COMMISSION



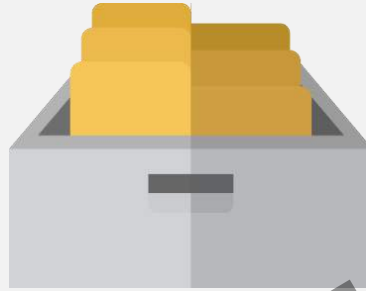
# LEGITIMATE PURPOSE



## *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.

THE FIVE

Pillars

OF  
Compliance

PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION





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



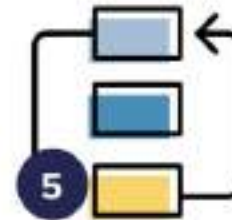
Know Your Risks:  
Conduct a **Privacy Impact Assessment** (PIA).



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).



## ***The Importance of a Data Protection Officer***






The  
**champion**  
**of privacy**  
within your  
organization.

Your  
**point of**  
**contact** for  
data subjects  
and the NPC.

DPO



# ***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?

# THE NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK



## I. GOVERNANCE

A. Choose a DPO



## II. RISK ASSESSMENT

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



## III. ORGANIZATION

E. Privacy Management Program  
F. Privacy Manual



## IV. DAY TO DAY

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



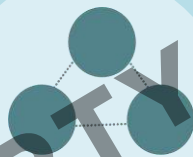
## V. DATA SECURITY

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



## VI. BREACHES

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



## VII. THIRD PARTIES

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



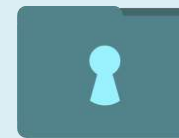
## VIII. MANAGE HR

V. Trainings and Certifications  
W. Security Clearance



## IX. CONTINUITY

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



## X. PRIVACY ECOSYSTEM

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

13. Policies/procedures for accepting and addressing complaints from data subjects

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.

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

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

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

## V. Managing Personal Data Security Risks

17. Implement appropriate and sufficient organizational security measures (Policies and procedures in place)

18. Implement appropriate and sufficient physical security measures (Physical Access and Security, Design and Infrastructure)

19. Implement appropriate and sufficient technical security measures (Firewalls, Encryption, Access Control Policy, Security of Data Storage, and Other Information Security Tools)

## VI. Data Breach Management

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

# Data Privacy Act Checklist

## Data Privacy Act (RA 10173) Checklist

Signs of Compliance, Commitment to Comply, Capacity to Comply

vs.

Signs of Negligence

### Pillar 1: Commit to Comply: Appoint a Data Protection Officer (DPO)

Sec. 21 of the DPA, Section 50 of the IRR, Circular 16-01, and Advisory 17-01

Appoint an individual accountable for compliance	Ineffective data protection governance
<ul style="list-style-type: none"> <li><input type="checkbox"/> Notarized designation of a DPO/COP, filed with the NPC</li> <li><input type="checkbox"/> Evidence that DPO/COP recommendations are taken into consideration when making decisions</li> <li><input type="checkbox"/> Contact details are easy to find (e.g. on website)</li> <li><input type="checkbox"/> Continuing education program for the DPO/COP</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> No DPO or COP (in which case CEO or HoA is the default DPO)</li> <li><input type="checkbox"/> Lack of interaction between DPO/COP and top management</li> <li><input type="checkbox"/> Lack of interaction between DPO/COP and functional units</li> <li><input type="checkbox"/> Communication from the DPO/COP is largely ignored</li> <li><input type="checkbox"/> No continuing education program for the DPO/COP</li> </ul>

### Pillar 2: Know Your Risks: Conduct a Privacy Impact Assessment (PIA)

Sec. 20(c) of the DPA, Section 29 of the IRR, Advisory 17-03

Know the risks represented by the processing to the rights and freedoms of data subjects	Data processing controls do not take into account the risks to the rights and freedoms of data subjects
<ul style="list-style-type: none"> <li><input type="checkbox"/> Up-to-date organizational inventory of processes that handle personal data, including the list of process owners</li> <li><input type="checkbox"/> PIAs have been conducted, and are owned and kept up-to-date by the process owner</li> <li><input type="checkbox"/> Stakeholders (those involved in the information life cycle) have been consulted as part of the PIA process</li> <li><input type="checkbox"/> PIA includes a privacy risk map, a list of controls, an implementation plan, and a monitoring/evaluation milestone</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> No PIAs</li> <li><input type="checkbox"/> Process owners do not "own" the PIAs</li> <li><input type="checkbox"/> PIAs are not updated when changes are made to the process, or to the technologies being used in the process</li> <li><input type="checkbox"/> Stakeholders are not consulted for the PIA</li> <li><input type="checkbox"/> Controls identified during the PIA are not implemented</li> </ul>



# The Data Privacy Golden Rule

If you Can't Protect It  
**Don't** Collect It.





PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION

**“Laws too gentle are seldom obeyed; too severe, seldom executed.”** *Benjamin Franklin*



# About the NPC

# Ang personal information mo parang pagmamahal lang.

AGE  
MARITAL STATUS  
ETHNICITY NATIONALITY  
PHILOSOPHICAL AFFILIATIONS  
FULL MAIDEN NAME OF MOTHER  
HEALTH EDUCATIONAL ATTAINMENT  
E-MAIL ADDRESS CONTACT NUMBERS PIN CODE PASSWORDS  
SOCIAL SECURITY NUMBER PASSPORT INFORMATION TAX RETURNS  
CURRENT HEALTH RECORDS GENETIC RECORDS POLITICAL STANCE  
LIKES WATCHING HAMSTER, CORGI, AND HIPHOP MUSIC VIDEOS  
DOWNLOADED ENTIRE SARAH GERONIMO DISCOGRAPHY  
DISLIKES CINNAMON, WEEKDAYS, AND STRICT BOSSES  
HAS THREE CHILDREN, TWO BOYS AND ONE GIRL  
LIKES POSTING ABOUT #MATCHY, MATCHY.  
CONNECTS TO THE INTERNET VIA 3G  
WORKS AT EDI SA PUSO MO.  
VISITED HONG KONG  
LIFE PEGS  
SEARCH

Dapat sa tamang tao napupunta.





# SITH HAPPENS

...But that's what we were made to handle.  
For #DataPrivacy concerns and complaints,  
e-mail us at [complaints@privacy.gov.ph](mailto:complaints@privacy.gov.ph).





National Privacy Commission

April 29 at 12:30pm · 🌐

Bes, sayang ang bago mong cellphone kung kay dali naman pala ma-hack. Sundan ang mga expert tip na ito para lalong maprotektahan ang sarili tuwing gumagamit ng cellphone!

#PrivacyPH #DataPrivacy



Cell phone security: 30 expert tips to secure your smartphone

Keeping your data secure on your smartphones is critical, so we reached out to a...

TDCROCKS.COM



National Privacy Commission

April 19 at 1:32pm · 🌐

'Wag magpaloko. Sebi nga ng Facebook quiz na kamukha mo si James Reid, pero mag-ingat. Baka naman laal kinukuha na nile ang personal information mo.

Alarin kung paano pa mabain ang sarili sa internet:

[https://www.facebook.com/pg/privacy.gov.ph/photos/...](https://www.facebook.com/pg/privacy.gov.ph/photos/)

#WagmahaPisakitSaHack #PrivacyPH #DataPrivacy



Hackers using Facebook quizzes to get your personal info

Hackers are using Facebook quizzes to trick people into providing personal...

PHILIPPINES





NATIONAL  
PRIVACY  
COMMISSION

2017 Edition  
Revised from 2015  
Version 4.0 - Privacy Data Act

# NPC Privacy Toolkit

A Guide for Management & Data Protection Officers

April 5, 2017



Kung hindi tayo kailas, sino ang sikat? Kung hindi ngayon, kailan pa?



NATIONAL  
PRIVACY  
COMMISSION

PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION







I WANT TO  
**Know More**

Know Your Rights

The Data Privacy Act and Its IRR

Memorandum Circulars



I WANT TO  
**Comply**

Register

Appointing a Data Protection Officer

Conducting a Privacy Impact Assessment



I WANT TO  
**Complain**

Mechanics

Submit a Complaint





# 2017 DATA PROTECTION OFFICERS (DPO) SUMMIT

**DPO Assembly For the Government Sector, Landbank of the Philippines, Manila, April 5, 2017 (347 participants)**



CONFIDENTIAL



**DPO Assembly For the Banking Industry, BSP Assembly Hall, Bangko Sentral ng Pilipinas, Pasay City, May 31, 2017 (129 participants)**



**DPO Assembly For Telecommunication Industry, GT-Toyota Asian Center Auditorium, University of the Philippines- Diliman, Quezon City, August 1, 2017 (181 participants)**





# STH HAPPENS

...But that's what we were made to handle.  
For #DataPrivacy concerns and complaints,  
e-mail us at [complaints@privacy.gov.ph](mailto:complaints@privacy.gov.ph).





presents



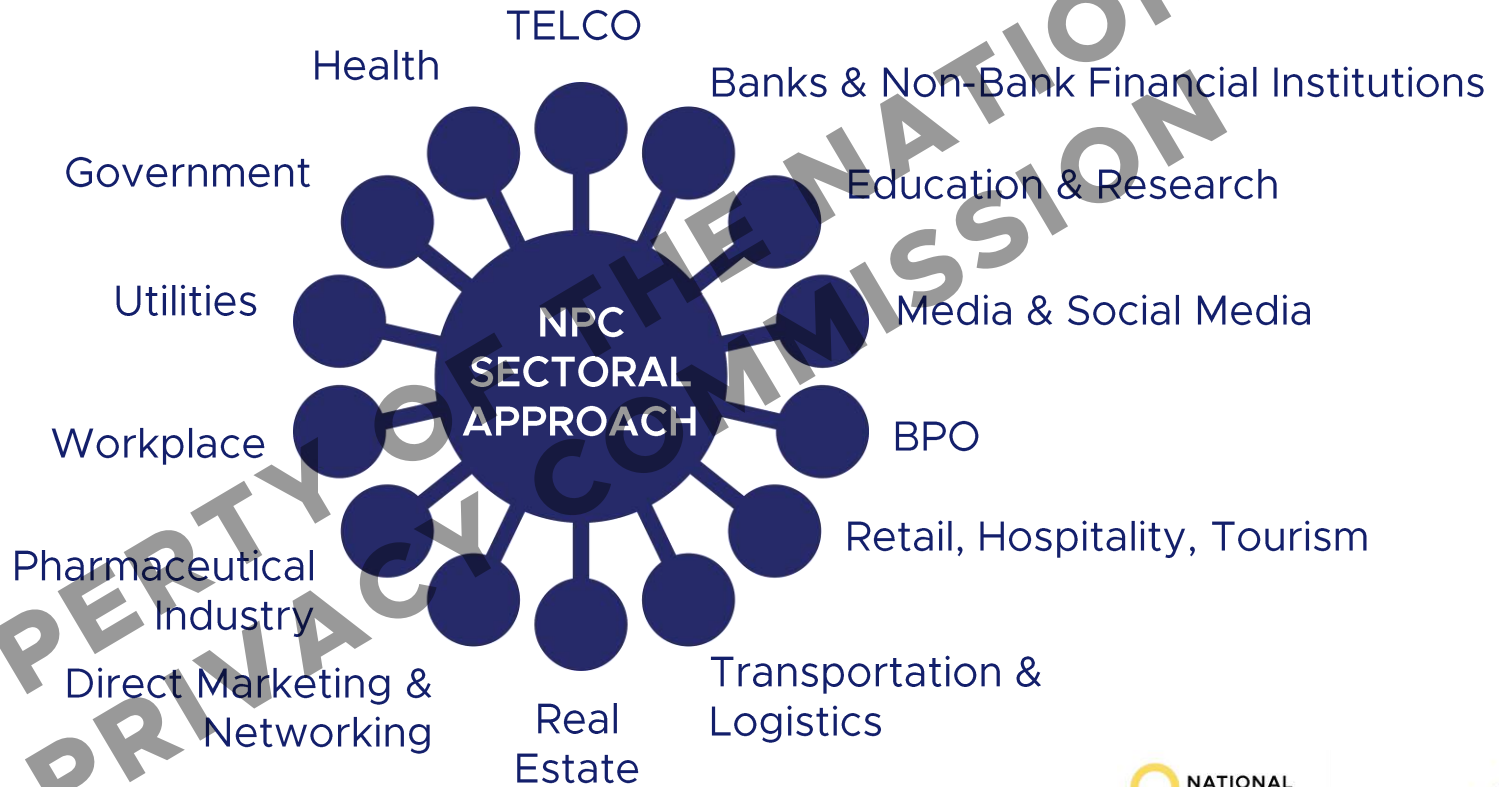
PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION

f [privacy.gov.ph](https://www.privacy.gov.ph)    t [privacyPH](https://twitter.com/privacyPH)





# NPC SECTORAL APPROACH





# ***Building Resiliency. Enforcing the Data Privacy Act***



PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION

**COMPLIANCE**  
doing what's required

**ACCOUNTABILITY**  
doing what's necessary



PROPERTY OF THE NATIONAL  
PRIVACY COMMISSION

**COMPLIANCE**  
blind trust

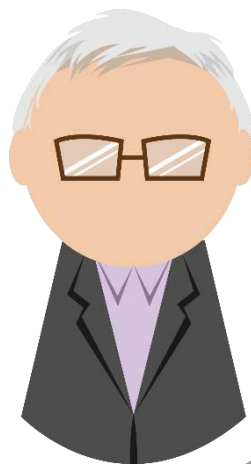




**ACCOUNTABILITY**  
proven trust







**PRIVACY.GOV.PH**

[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)

920-0101 (Local)

7001 OPC

7021 PIAD

7041 CMD

