

.....

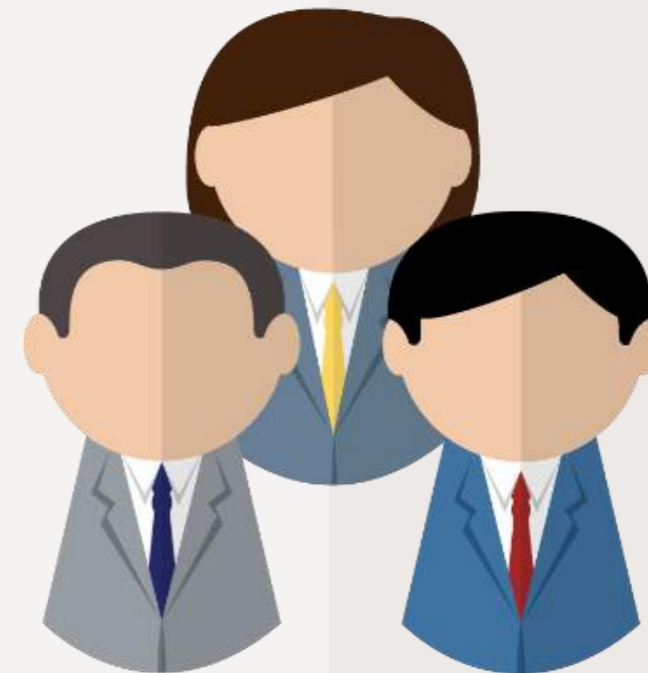
The Data Privacy Act of 2012 Impact and Significance To the Retail Industry

.....

RAYMUND ENRIQUEZ LIBORO
PRIVACY COMMISSIONER AND CHAIRMAN



What the **law** is
all about

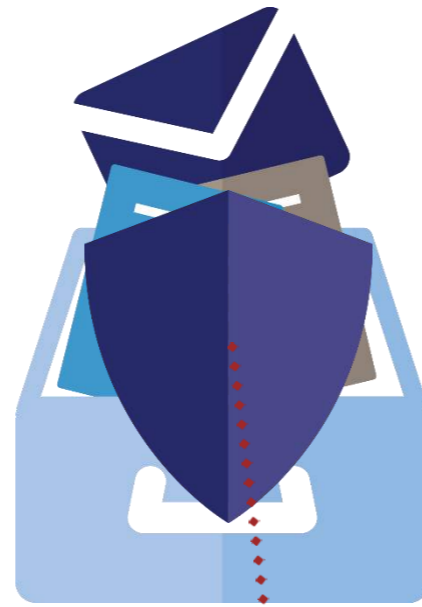


How it will
affect **you**

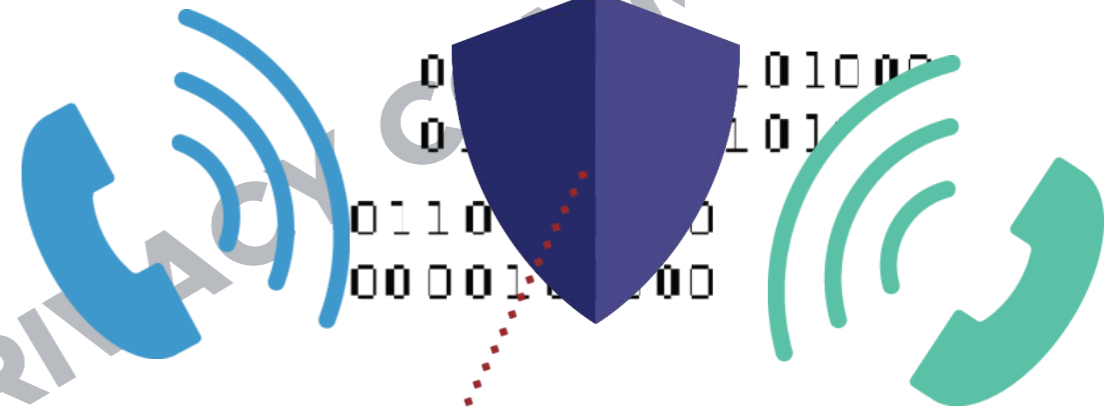
Information Privacy Then...



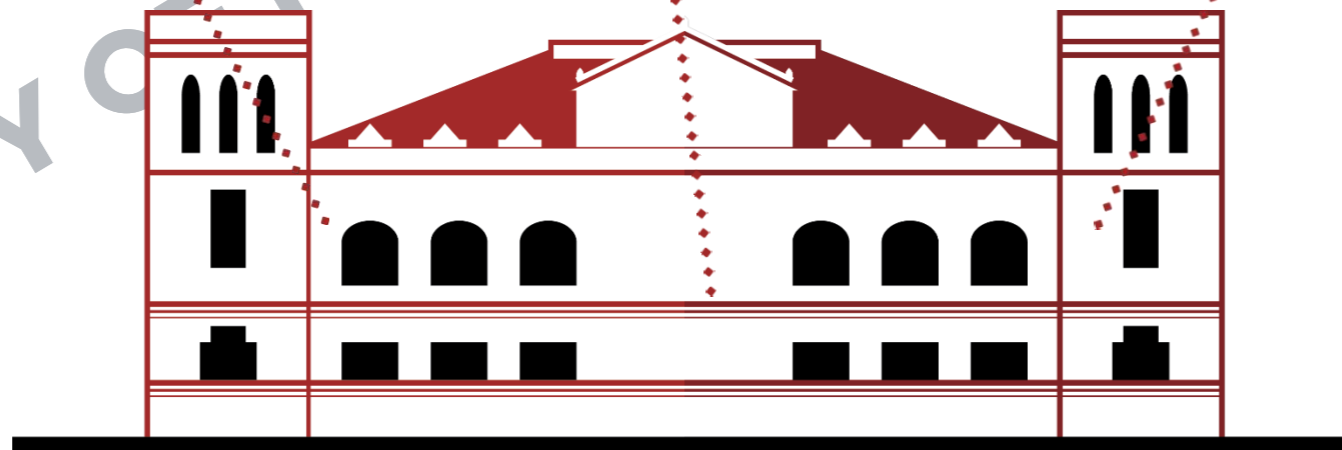
Persons, houses,
papers, and effects



Correspondence



Communication

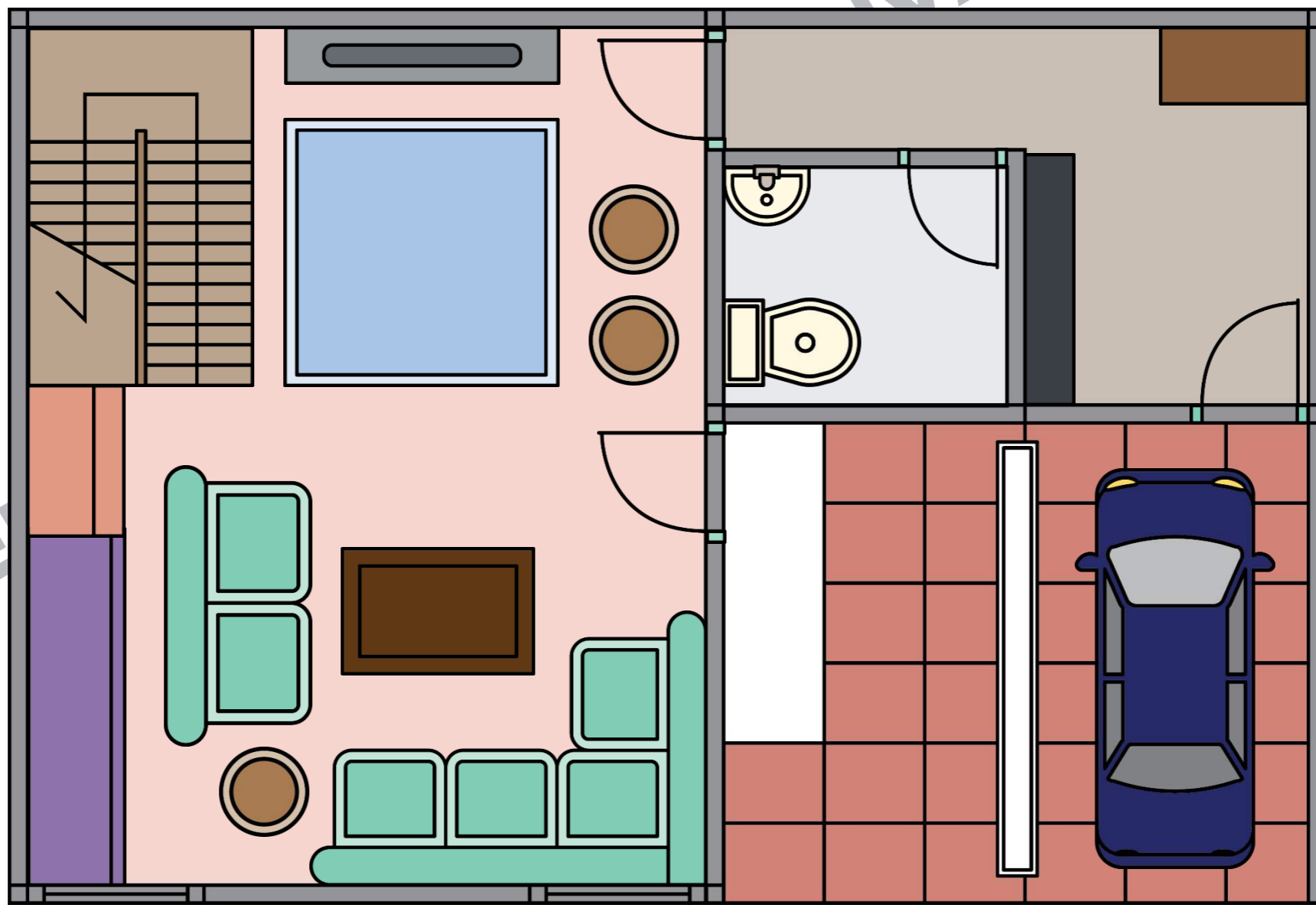


protected from government intrusions
through **illegal searches**

PROPERTY OF NATIONAL PRIVACY COMMISSION

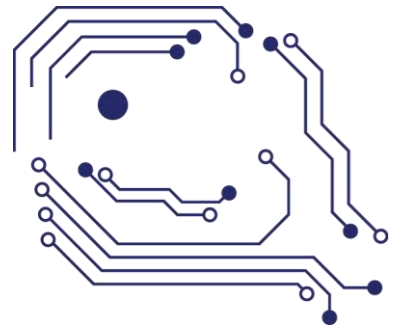
What is private then

was what was found within the four corners of your **home** and within the confidentiality of communication.



PROPE

WACY COMMISSION

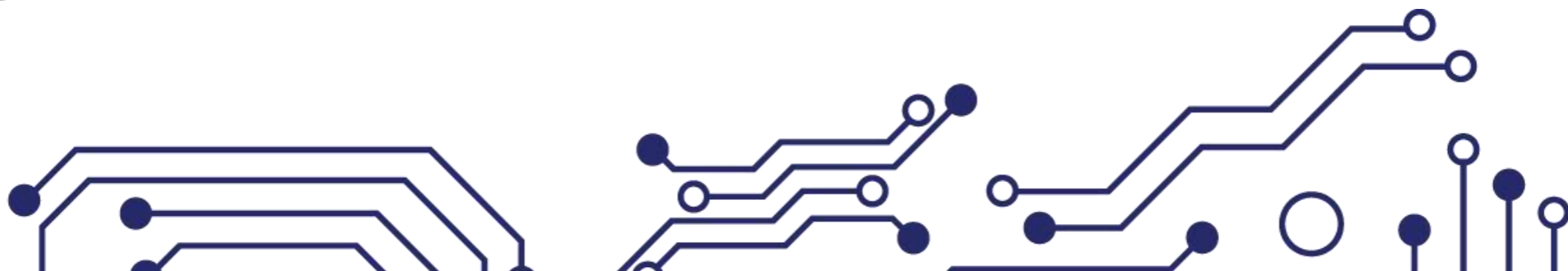


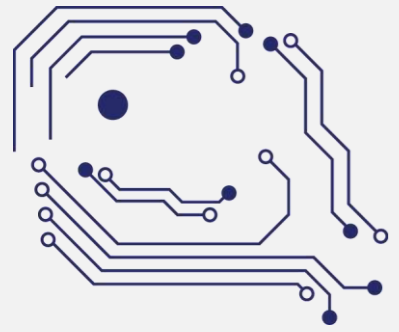
Shift of Perspective

From the **household** to a **reasonable expectation of privacy**

What a person knowingly exposes to the public, even in his own house or office, is not what is private,

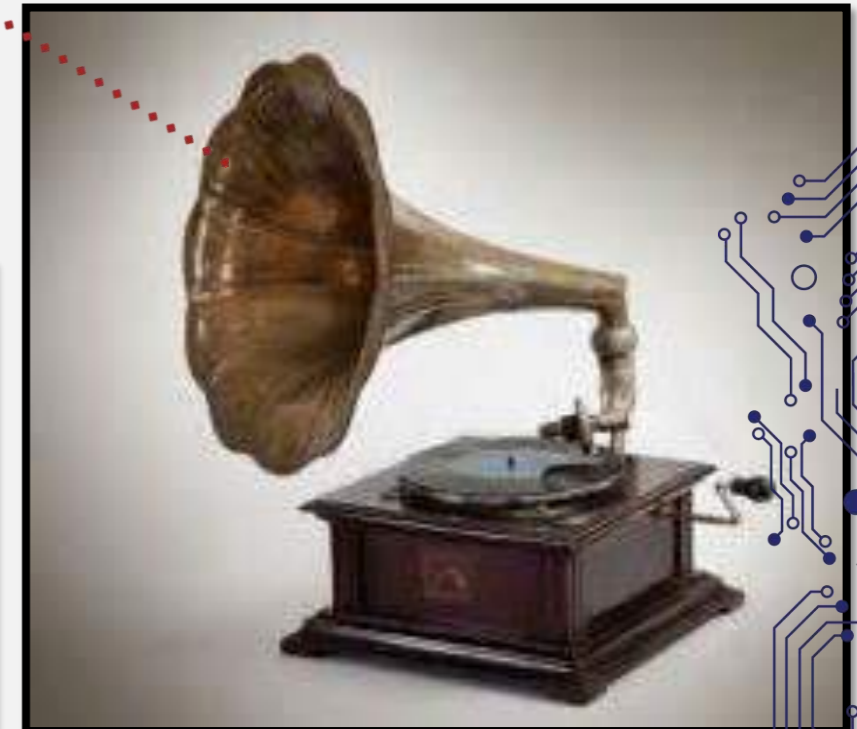
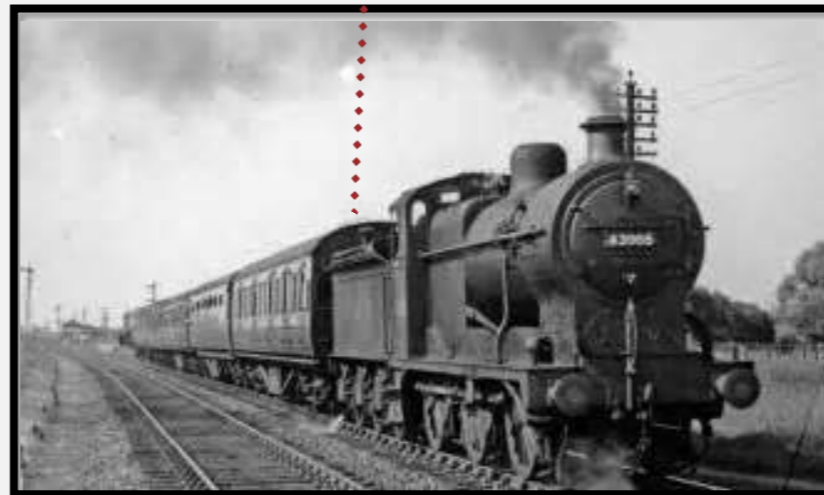
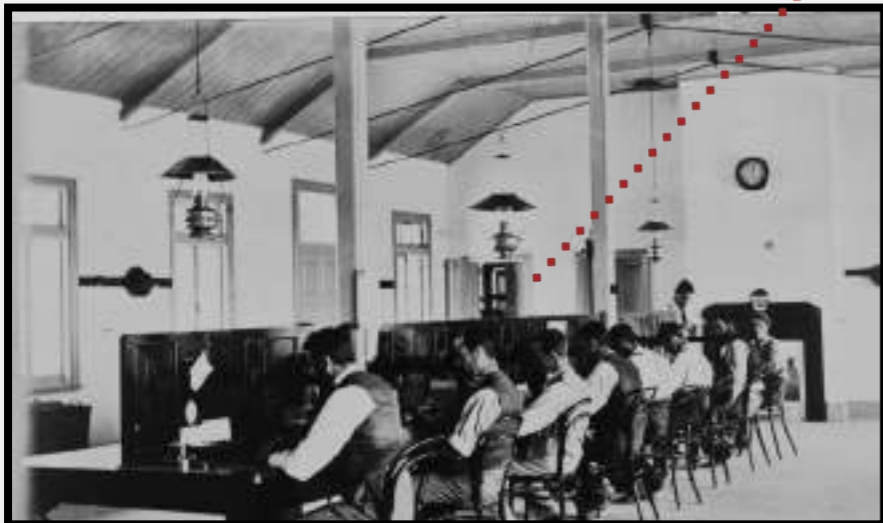
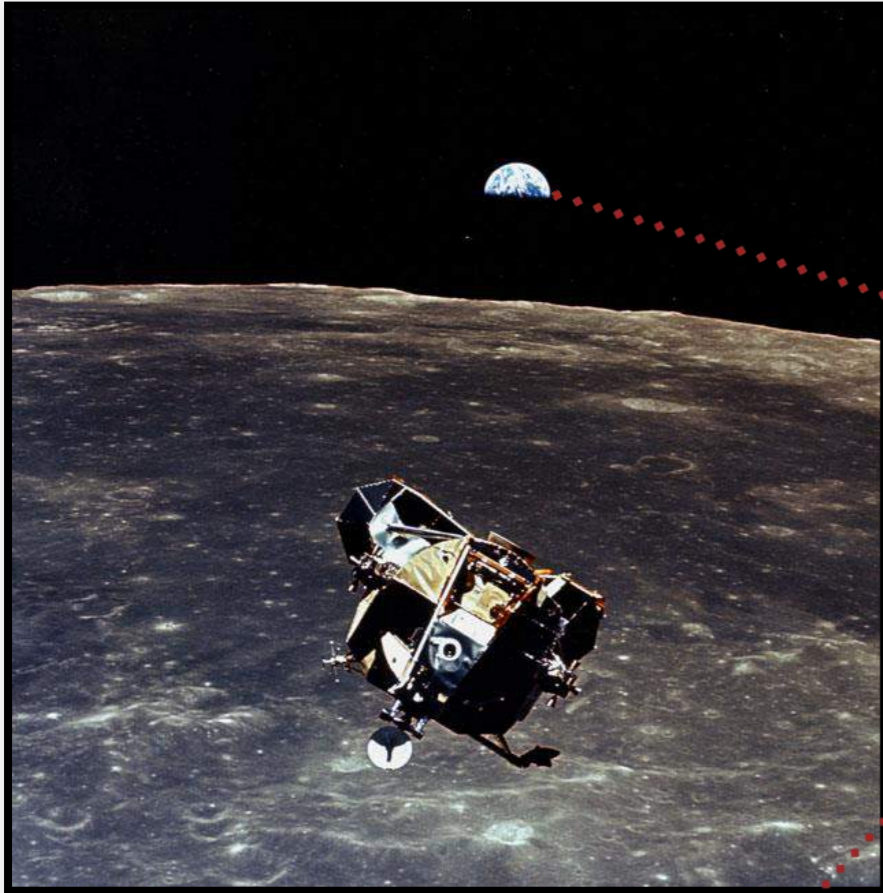
But what he seeks to preserve as private, even in a public area.



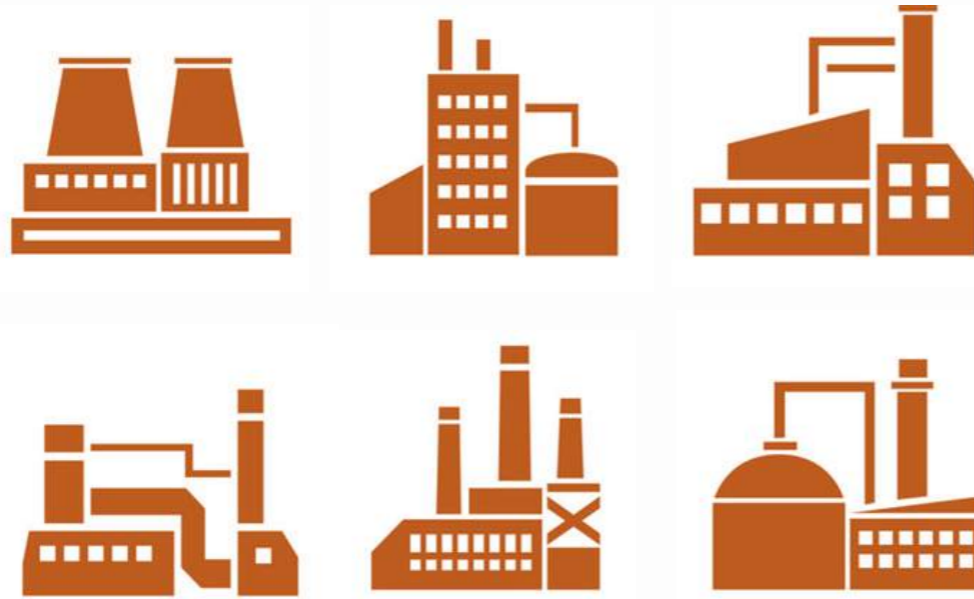


The Information Age

The Dramatic Change in Technology



From *Industrial Revolution*

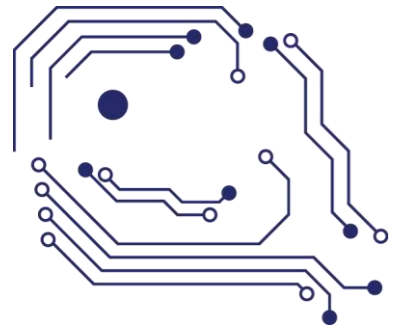


To *Information Revolution*



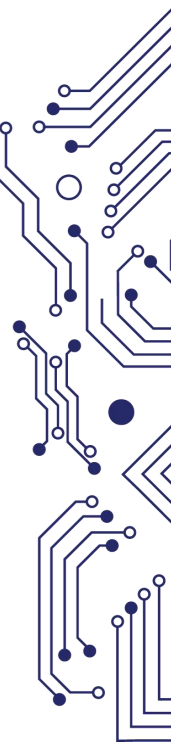
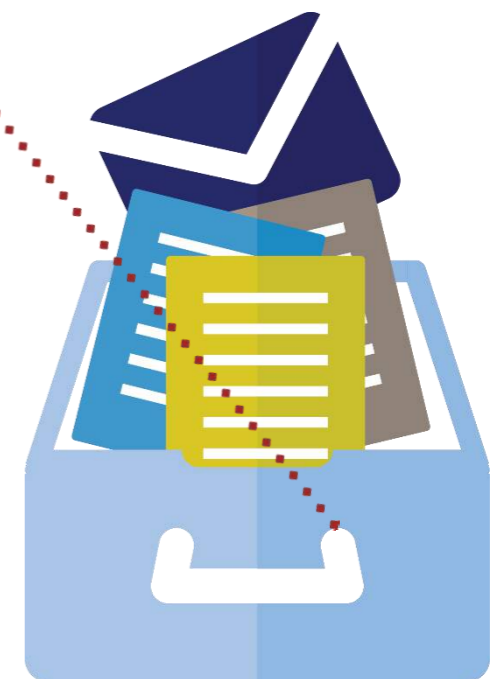
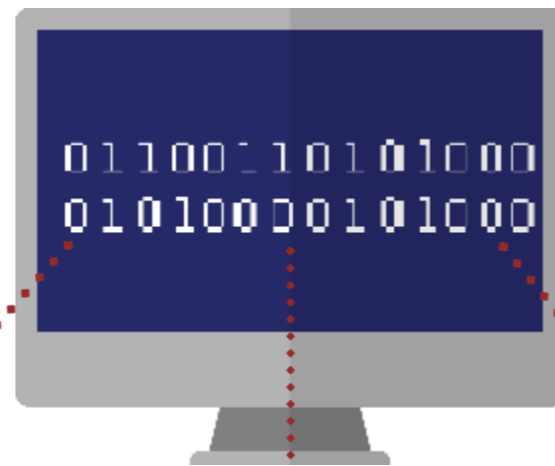
PROPER™

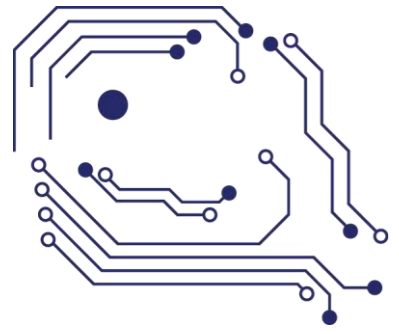
CONFIDENTIAL PRIVACY COMMISSION



The Information Age

The Info Structure Environment



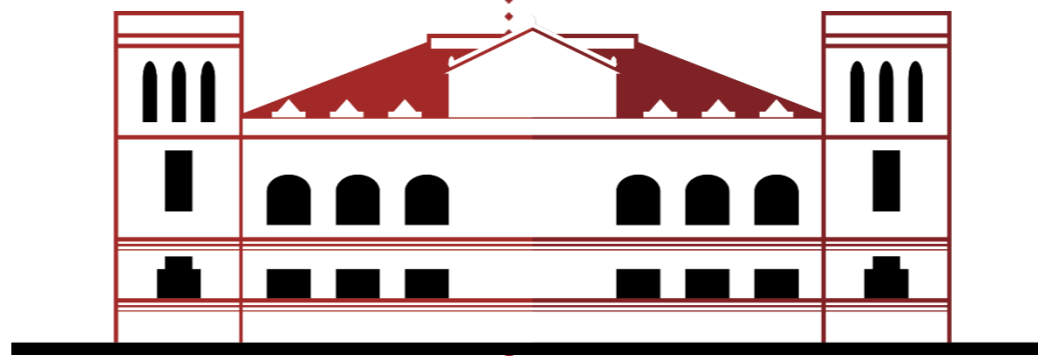


The Information Age

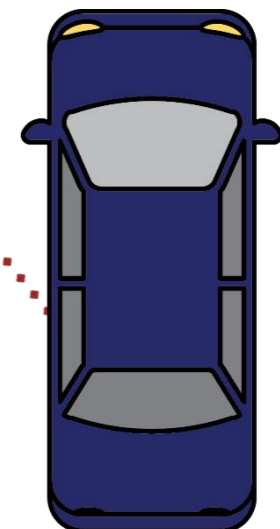
The Info Structure Environment



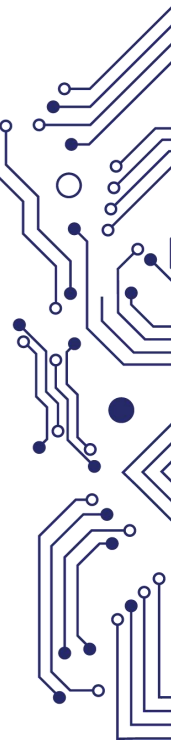
Better Healthcare

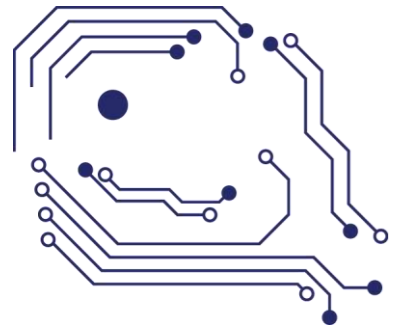


Better Govt.



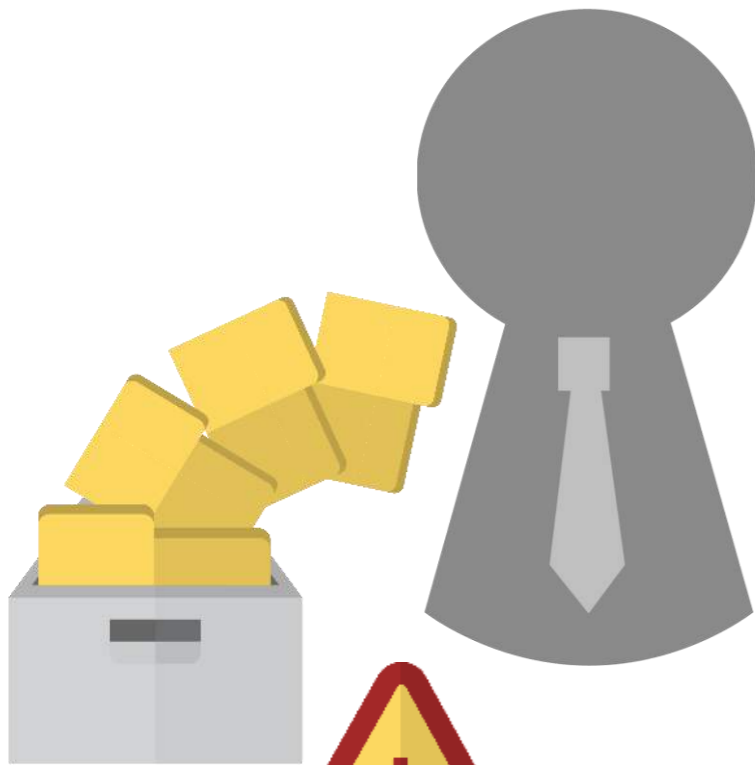
Better Transp.



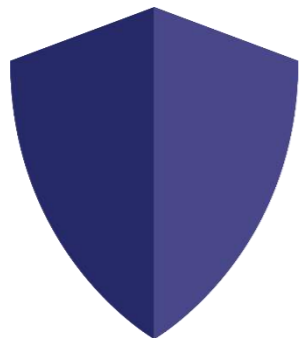


The Information Age

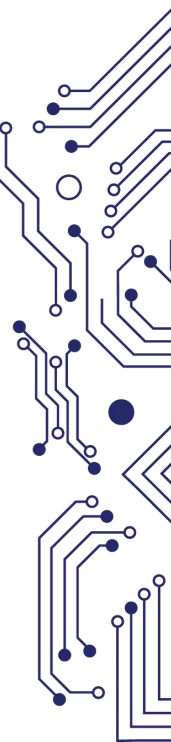
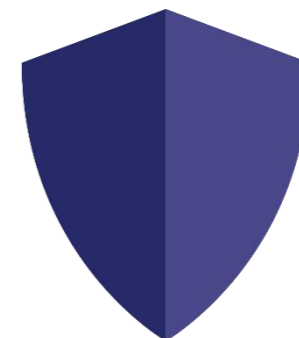
Potential Dangers



Internal



External



The Product of a 21st Century Law



**NATIONAL
PRIVACY
COMMISSION**



For Addressing 21st Century Concerns

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

1995

SSION



2015

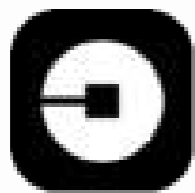
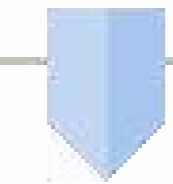


The world's largest taxi company, owns **no vehicles.**

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

Technology eliminates the *Middleman*



DATA
as the common
Denominator

Forbes Most Valuable Brands 2007 versus 2017

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

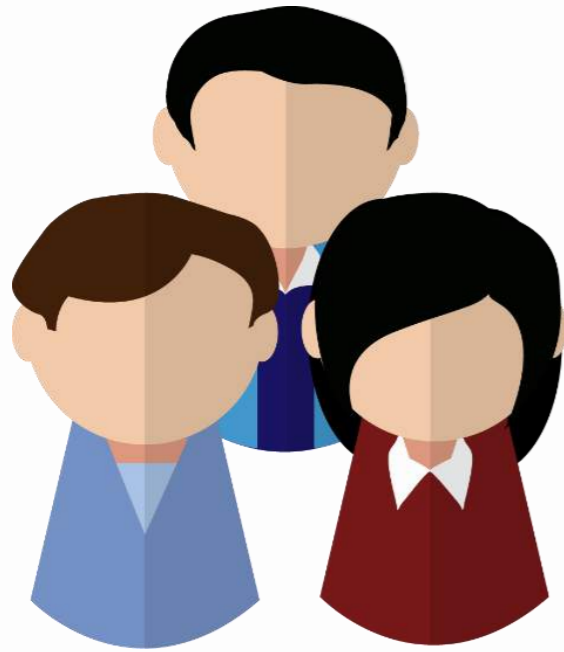


McDonalds



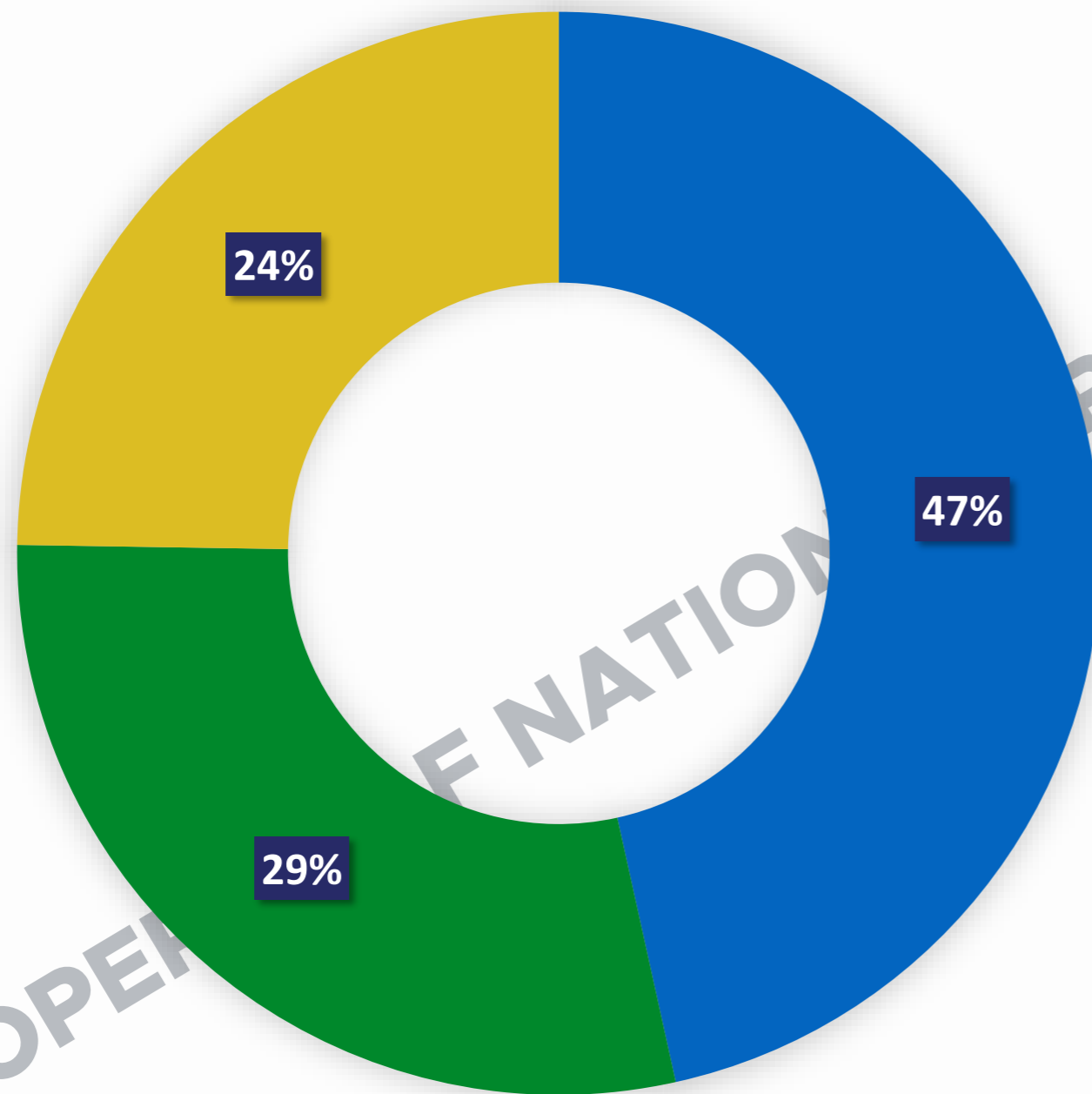
Samsung

Impact of a Problematic Data Action on Business



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

ROOT CAUSES OF BREACH



■ Malicious or criminal attack

■ System Glitch

■ Human Error

Key Statistics

88%

Vulnerable – 19% very or extremely vulnerable

52%

Had a data breach overall – 19% in the last year, and 11% more than once

77%

Increasing IT security spending. Up from 61% in 2016 and 62% in 2015

88 percent of retailers vulnerable to data breaches in 2017

By Retail Tech Innovation editors | 2017-08-01

[Email](#) [Print](#) [Share](#)

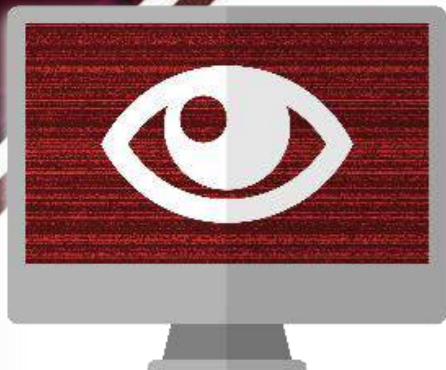


The 2017 Thales Data Threat Report, Retail Edition revealed that 43% of retailers had experienced a data breach in the last year with 32% claiming a breach occurring more than once. Produced in conjunction with analyst firm 451 Research also revealed that 88% of retailers consider themselves vulnerable to data threats past year.

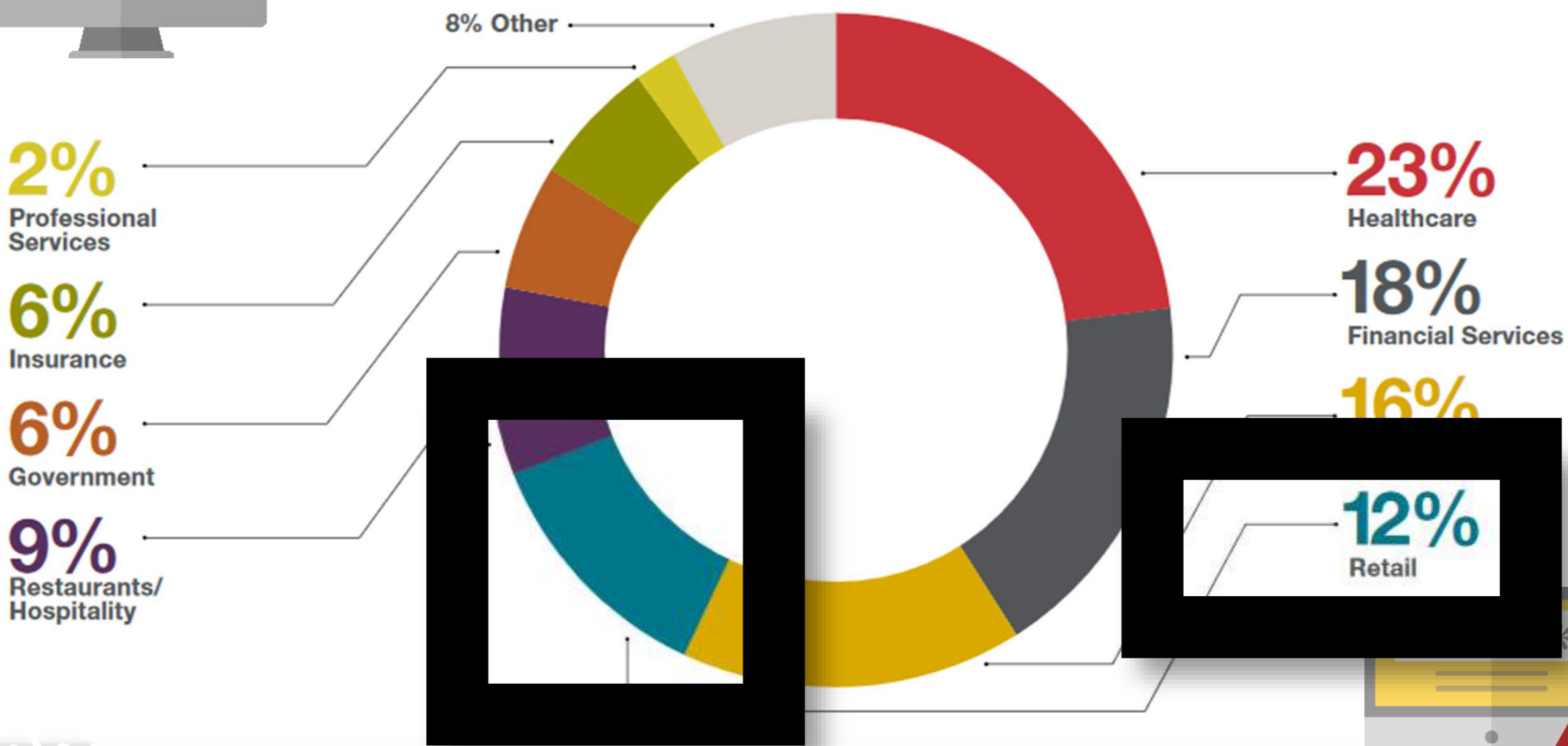
THALES

2017 Thales Data Threat Report
Retail Edition





Industries Affected



HOW DO PRIVACY BREACHES OCCUR

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



Retailers tracking customer return data prompts concerns over transparency



Jennifer C. Kerr, The Associated Press
Published Sunday, August 11, 2013 8:33AM EDT

WASHINGTON -- It's not just the government that might be keeping tabs on you. Many retailers are tracking you, too -- or at least your merchandise returns.

The companies say it's all in the name of security and fighting fraud. They want to be able to identify chronic returners or gangs of thieves trying to make off with high-end products that are returned later for store credit.

HOW DO PRIVACY BREACHES OCCUR

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

February 21, 2014 • min read by [Christine DiGangi](#) Comments 0 Comments

The [Target data breach](#) has caused a lot of headaches — it has also been crazy expensive.

A new report from the [Consumer Bankers Association](#) estimates the cost of [replacing the credit and debit cards](#) compromised in the breach has exceeded \$200 million. That's just card-replacement costs reported by the CBA and the Credit Union National Association. Factor in the impact of fraudulent activity and costs to financial institutions not members of the CBA or CUNA, and the price tag on the Target data breach gets a lot higher.

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



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

<http://blog.credit.com/2014/02/target-data-breach-cost-banks-240-million-76636/>

<https://nakedsecurity.sophos.com/2014/09/19/home-depot-breach-totals-56-million-credit-cards-exposed-62-million-in-losses/>

19 SEP 2014 10

Cryptography, Data loss, Law & order, Malware

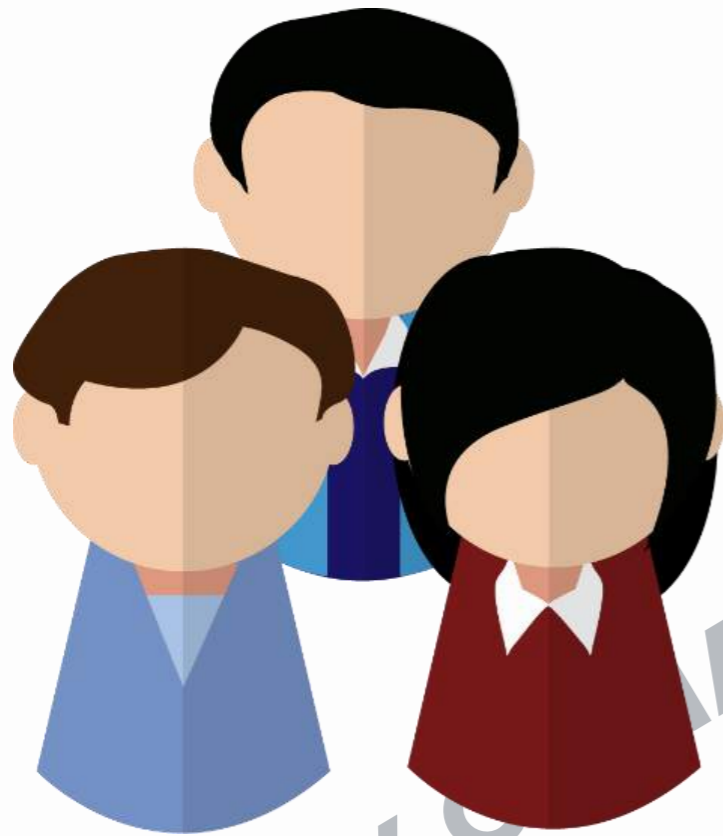


HOW DO PRIVACY BREACHES OCCUR

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

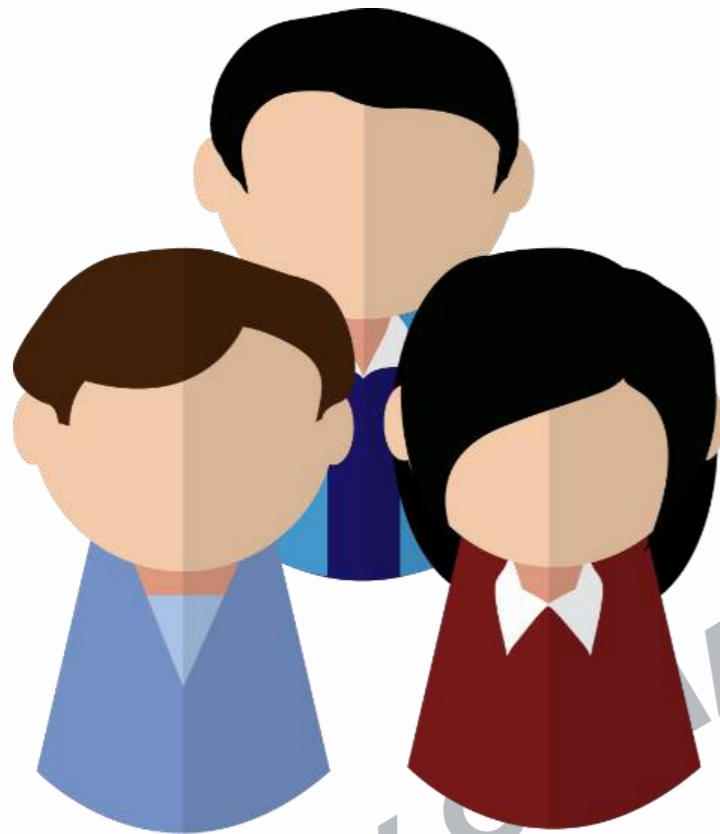


DATA PRIVACY RELATED DIFFICULTIES



- 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

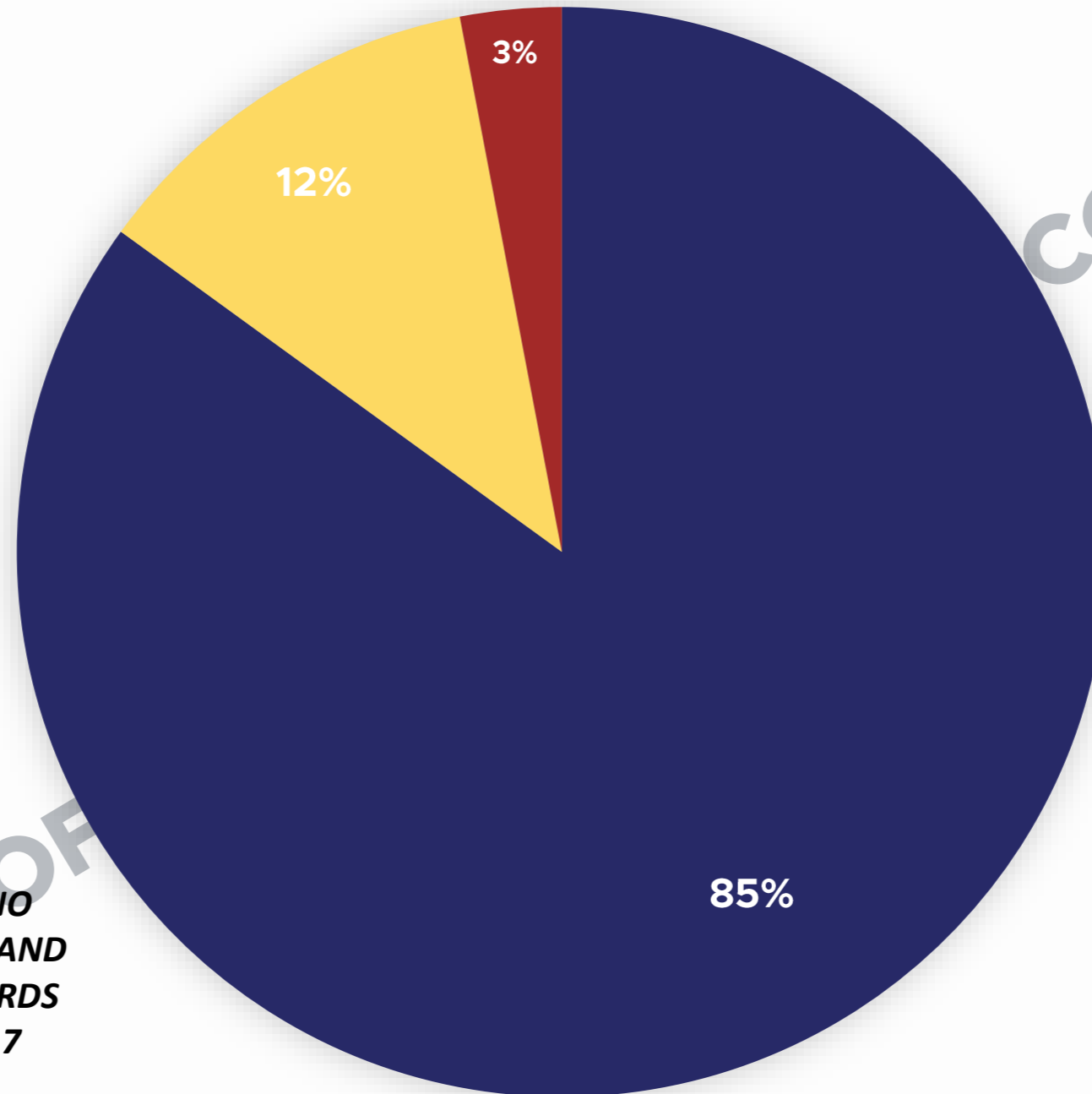


- Loss of trust
- Loss of self-determination
 - *Loss of autonomy*
 - *Loss of liberty*
 - *Exclusion*
 - *Physical harm*
- Discrimination
 - *Stigmatization*
 - *Power imbalance*
- Economic loss

Survey Results

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

**% of
Adults**



**Net*
+83**

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

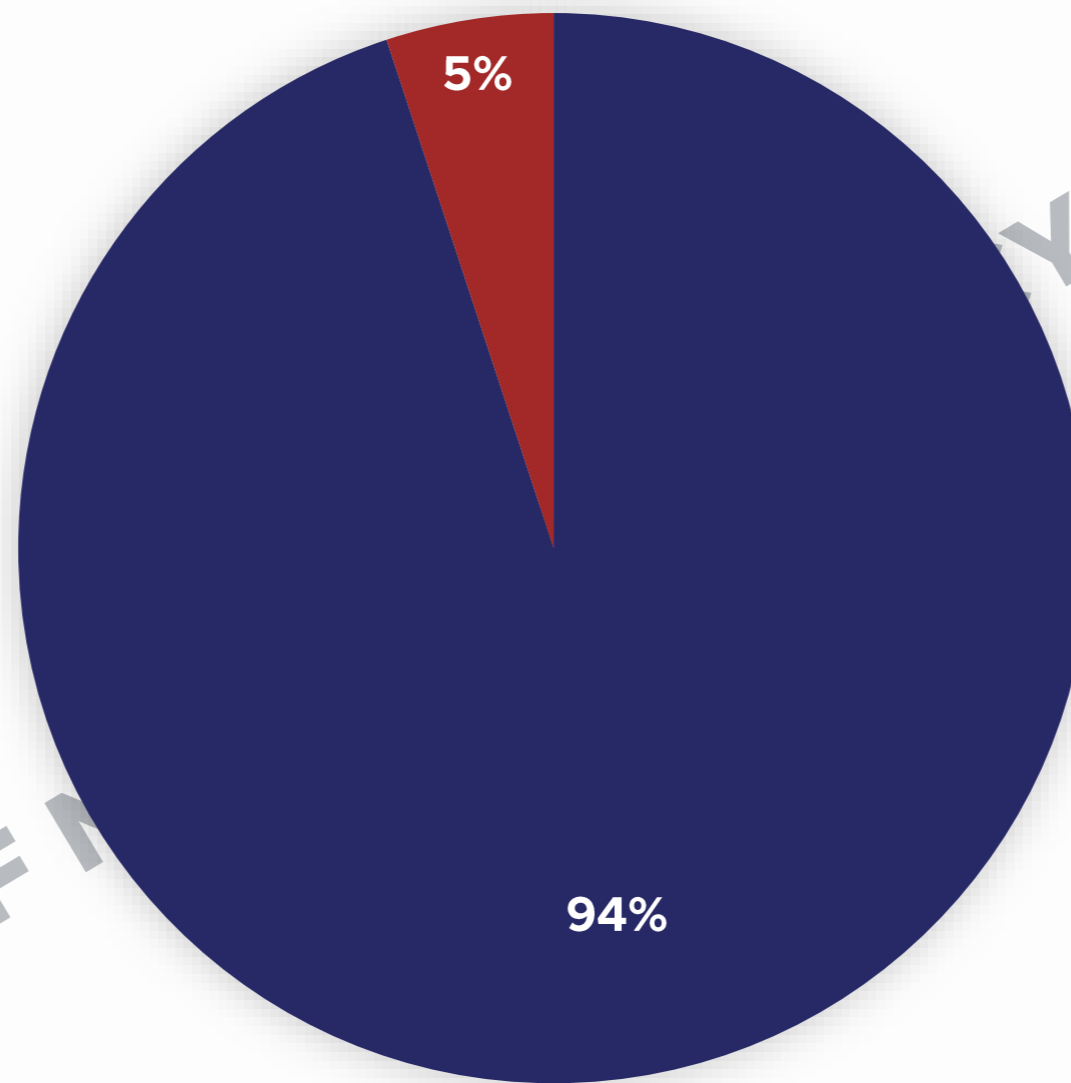
■ Important ■ Undecided ■ Not Important

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

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, June 2017

% of Adults



**Net*
+89**

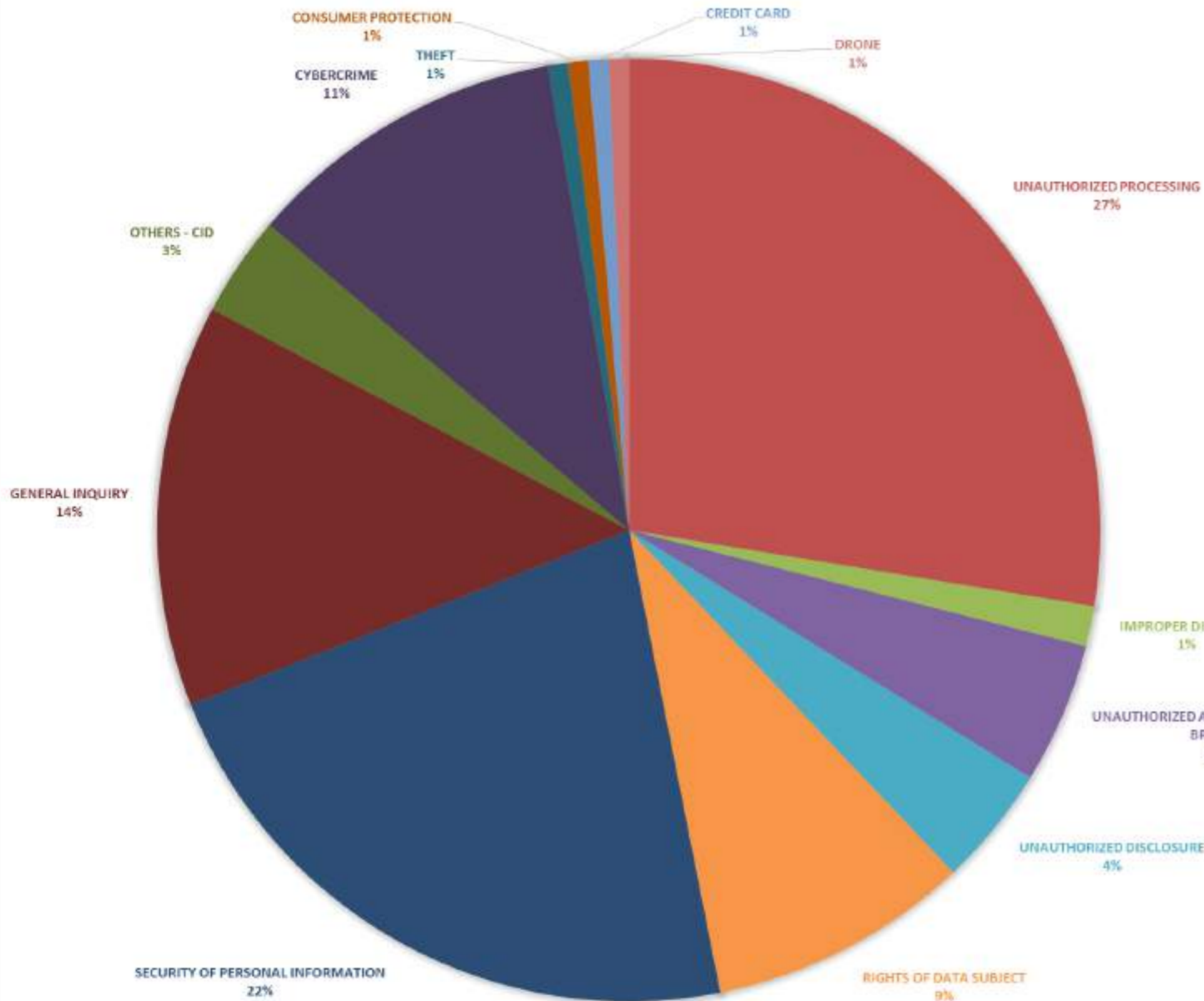
Based on the **SWS Survey "FILIPINO PUBLIC OPINION ON DATA PRIVACY AND ATTITUDES AND BEHAVIOUR TOWARDS INTERNET USAGE" June 17-21, 2017 National Survey*

■ Likes to Know ■ Does Not Like to Know

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

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

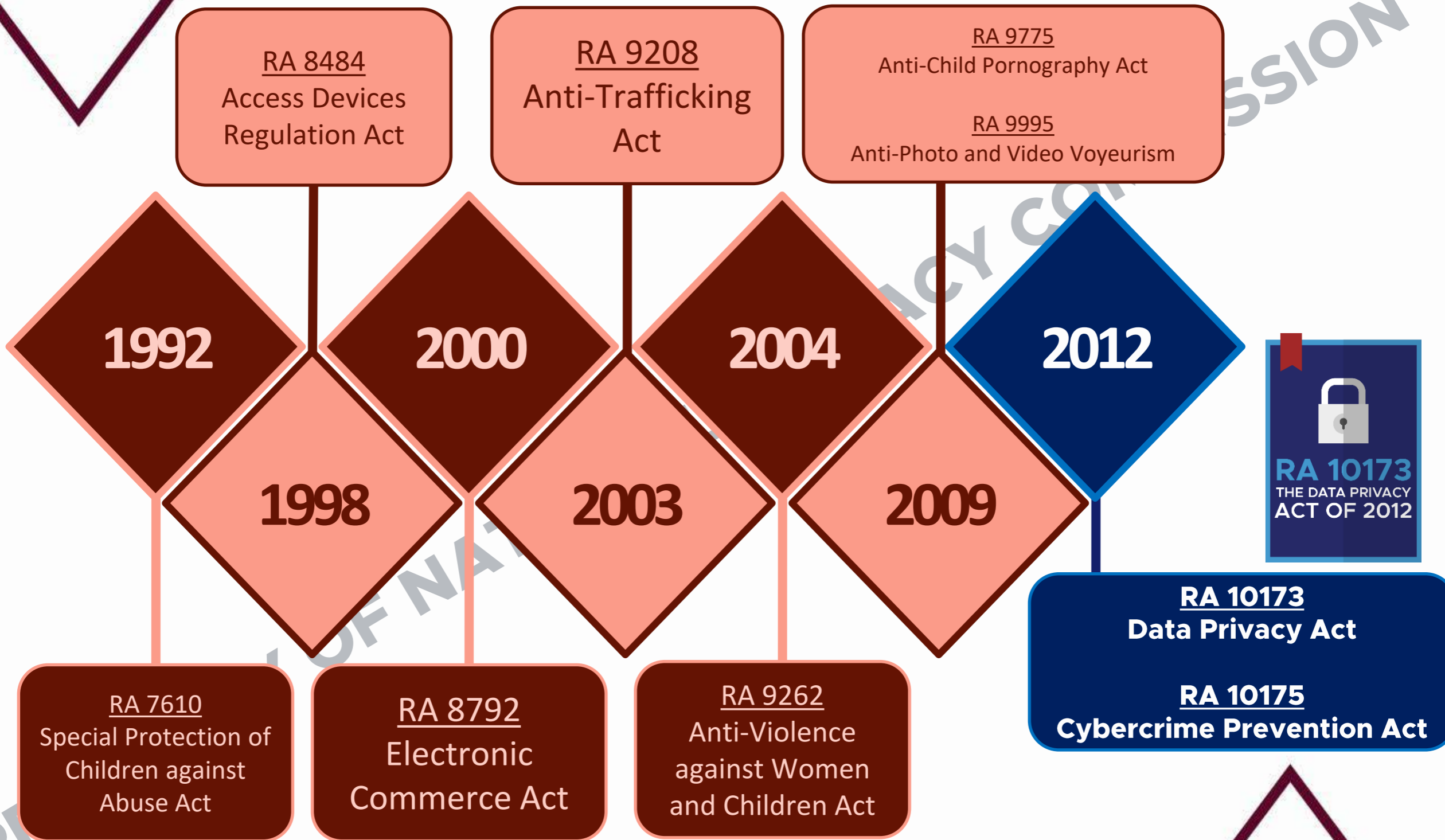
Nature of Complaints (as of August 31, 2017)



CLASSIFICATION	NO. OF COMPLAINTS	PERCENTAGE
UNAUTHORIZED PROCESSING	40	28%
IMPROPER DISPOSAL	2	1%
UNAUTHORIZED ACCESS/INTENTIONAL BREACH	7	5%
UNAUTHORIZED DISCLOSURE	6	4%
RIGHTS OF DATA SUBJECT	13	9%
SECURITY OF PERSONAL INFORMATION	32	22%
GENERAL INQUIRY	20	14%
OTHERS - CID	5	3%
CYBERCRIME	16	11%
THEFT	1	1%
CONSUMER PROTECTION	1	1%
CREDIT CARD	1	1%
DRONE	1	1%
TOTAL	145	100%



**NATIONAL
PRIVACY
COMMISSION**



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
.....




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***



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.**



Data Privacy

Free Flow

Information
Privacy

Research

National Security
and Public Safety

Right to
Information

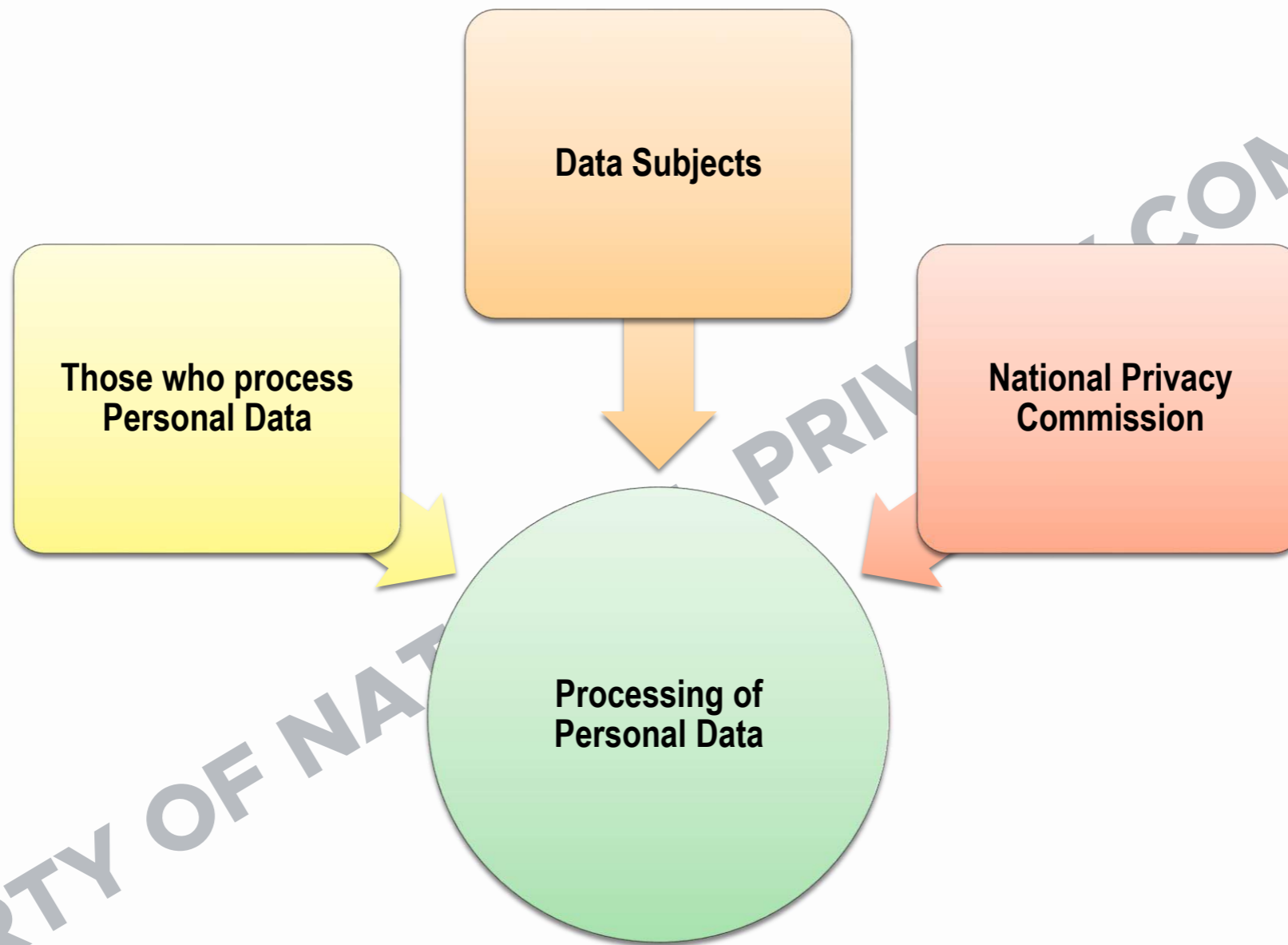
National Privacy Commission

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.



CREATE AND COLLECT



STORE AND TRANSMIT



DISPOSE AND DESTROY



THE DATA LIFE CYCLE

RETAIN



USE AND DISTRIBUTE



PROPERTY OF NATIONAL PRIVACY COMMISSION

I. CREATE AND COLLECT



Punishable Act

Imprisonment

Fine (PHP)

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



COMMISSION

Punishable Act	Imprisonment	Fine (PHP)
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



COMMISSION

Punishable Act

Imprisonment

Fine (PHP)

Improper Disposal of Records

6 months to 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



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.

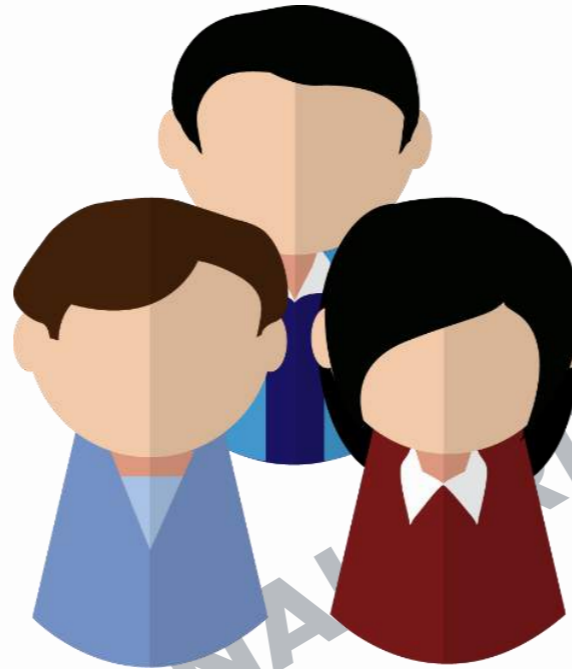


Data Privacy Principles

Security Measures

Uphold Rights of Data Subject

DATA SUBJECT



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

RIGHTS OF A DATA SUBJECT



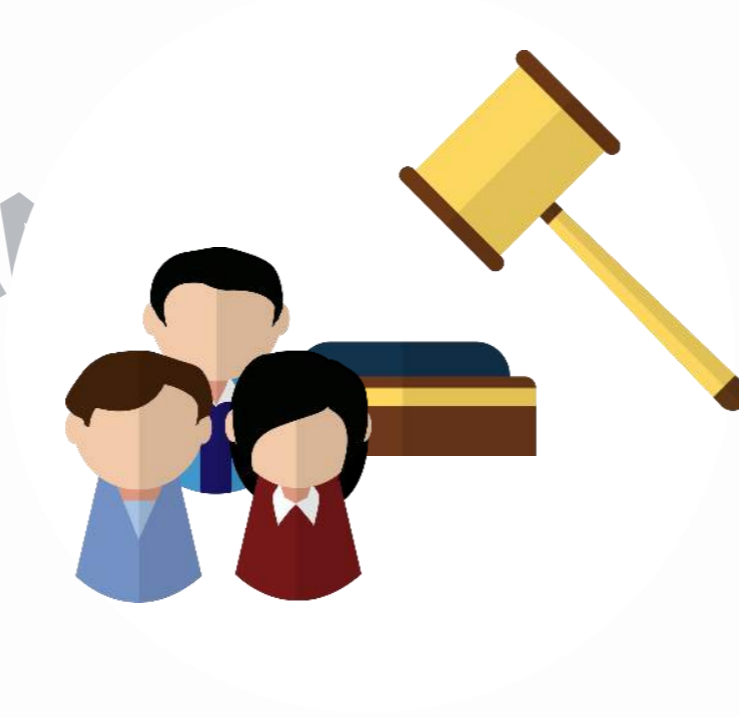
Right to be Informed



Right to Object



Right to Access



RIGHTS OF A DATA SUBJECT



**Right to
Correct/Rectify**

**Right to
Block/Remove**



**Right to Data
Portability**



RIGHTS OF A DATA SUBJECT



Right to File a Complaint

Right to be Indemnified





KEY CONCEPTS

CLASSIFICATION OF PERSONAL DATA



Personal Information:

Personal information refers to **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.**

Sensitive Personal Information

Refers to personal information about an individual's:

race, ethnic origin, marital status, age, color, religious, philosophical or political affiliations, health, education, genetics, sexual life, any proceeding for any offense committed or alleged to have been committed, the disposal of such proceedings, the sentence of any court in such proceedings;

Also includes information issued by government agencies peculiar to an individual which includes, but not limited to:

social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns;

and specifically established by an executive order or an act of Congress to be kept classified.



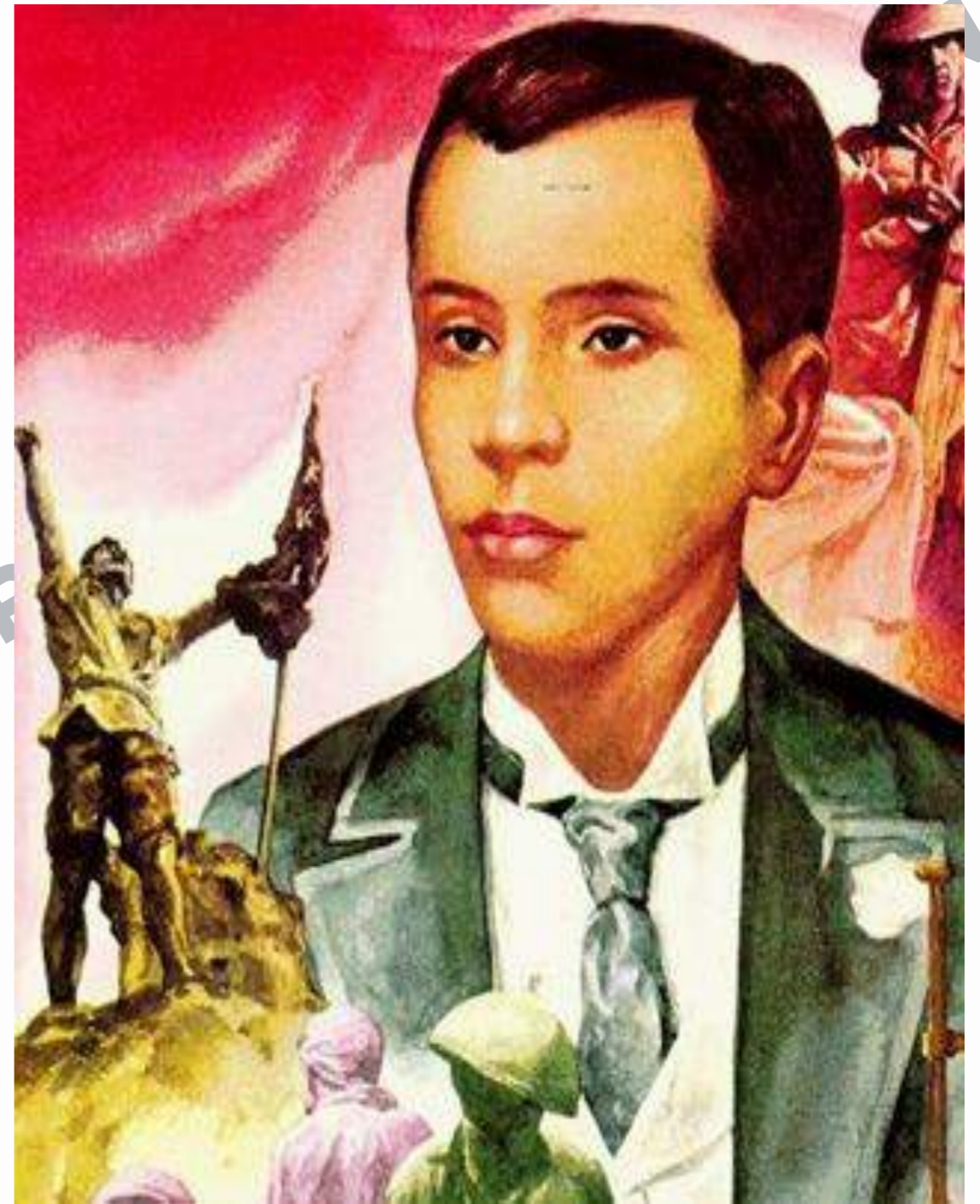
Personal Information	Sensitive Personal Information (List based on IRR)	Privileged Information (List based on Rules of Court)
Name	Race	Data received within the context of a protected relationship – husband and wife
Address	Ethnic origin	
Place of work	Marital status	
Telephone number	Age	
Gender	Color	Data received within the context of a protected relationship – attorney and client
Location of an individual at a particular time	Religious affiliation	
IP address	Philosophical affiliation	
Birth date	Political affiliation	
Birth place	Health	Data received within the context of a protected relationship – priest and penitent
Country of citizenship	Education	
Citizenship status	Genetics	
Payroll & benefits information	Sexual life	Data received within the context of a protected relationship – doctor and patient
Contact information	Proceeding for any offense committed or alleged to have been committed, the disposal of such proceedings, the sentence of any court in such proceedings	

	Sensitive Personal Information (List based on IRR)	
	<i>Social security number</i>	
	<i>Licenses or its denials, suspension or revocation</i>	
	<i>Tax returns</i>	
	<i>Other personal info issued by government agencies</i>	
	<i>Bank and credit/debit card numbers</i>	
	<i>Websites visited</i>	
	<i>Materials downloaded</i>	
	<i>Any other information reflecting preferences and behaviors of an individual</i>	
	<i>Grievance information</i>	
	<i>Discipline information</i>	
	<i>Leave of absence reason</i>	
	<i>Licenses or its denials, suspension or revocation</i>	

Which data is personal information?

D)

- A) November 30, 1863
- B) Filipino, male, born on November 30, 1863
- C) Philippine Hero, born on November 30, 1863



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.

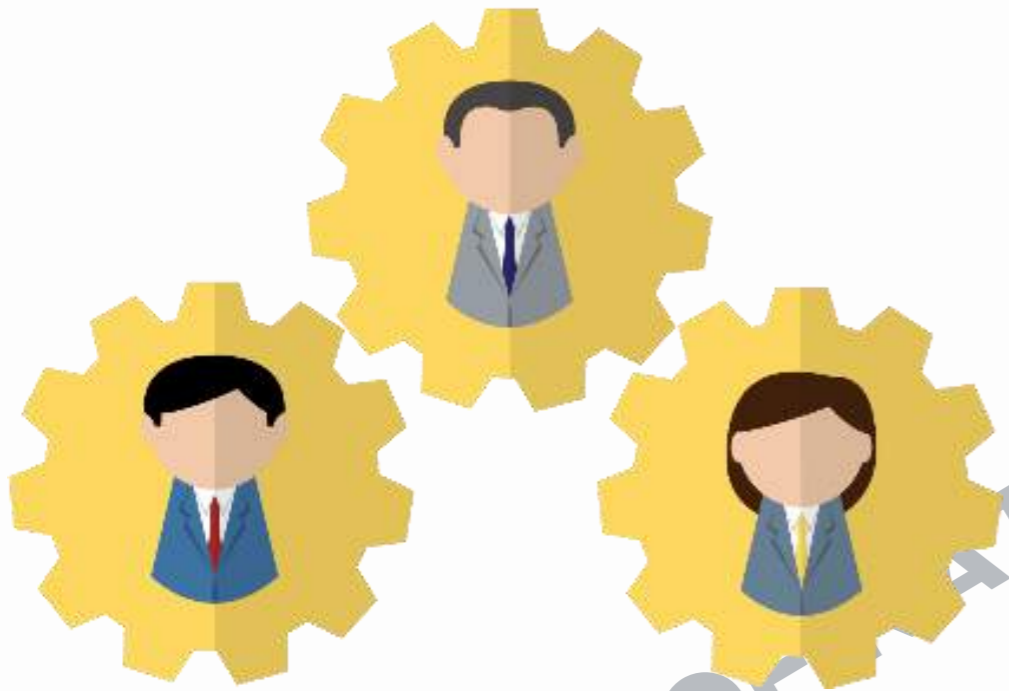
It excludes:

- ✂ 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.



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.

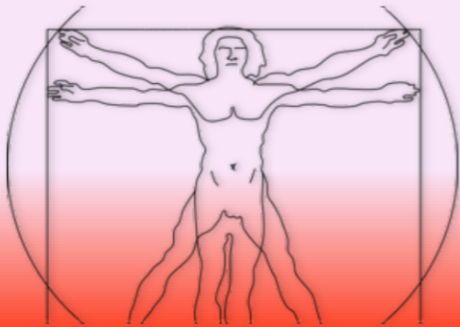
DATA PRIVACY PRINCIPLES

NOTICE

TRANSPARENCY



LEGITIMATE PURPOSE



PROPORTIONALITY

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**



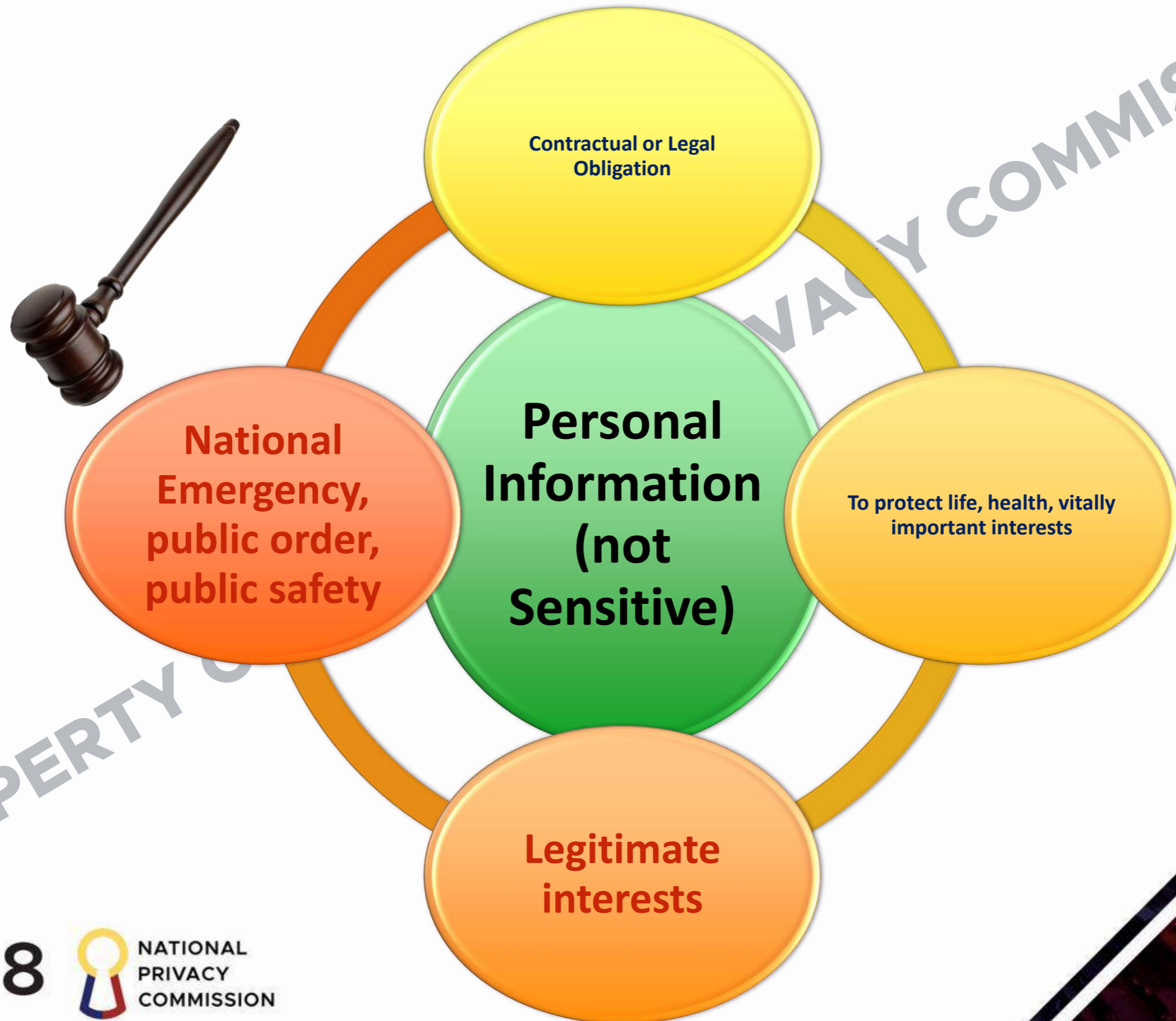
Consent of the data subject

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.

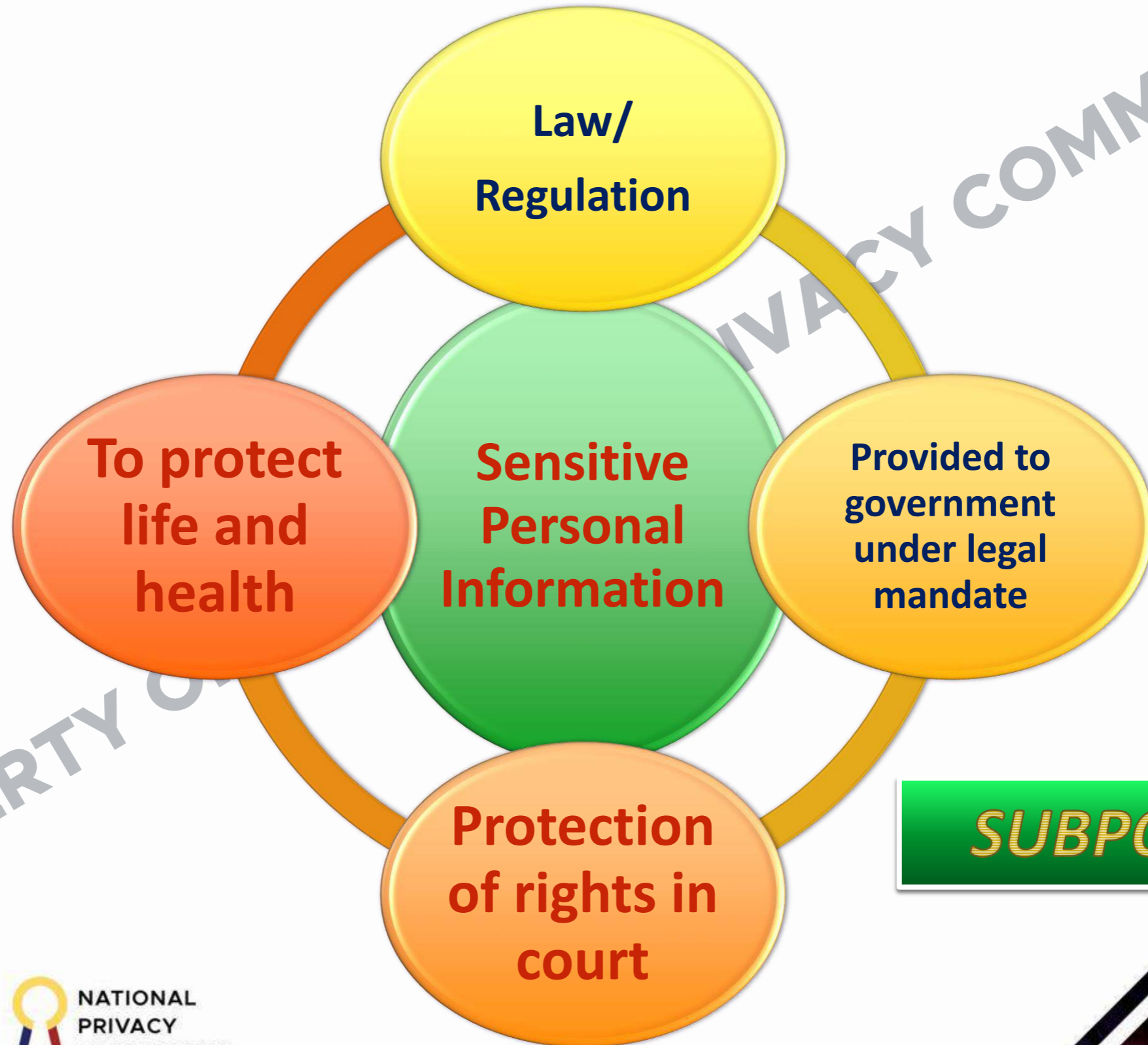
If It's **NOT CLEAR**

It's **NOT** Consent

Sometimes, consent is NOT necessary..



Sometimes, consent is NOT necessary...



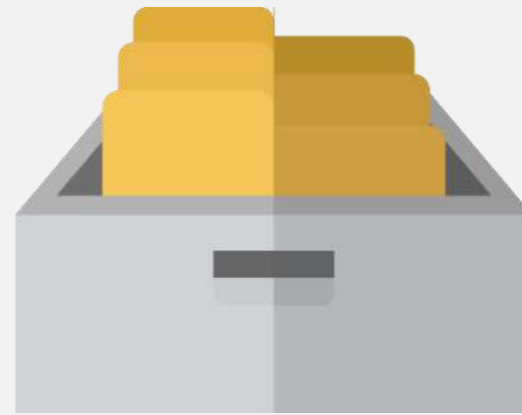
LEGITIMATE PURPOSE



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





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



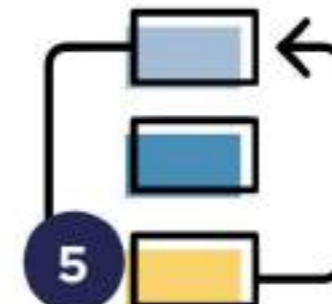
Know Your Risks:
Conduct a **Privacy Impact Assessment** (PIA).



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 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



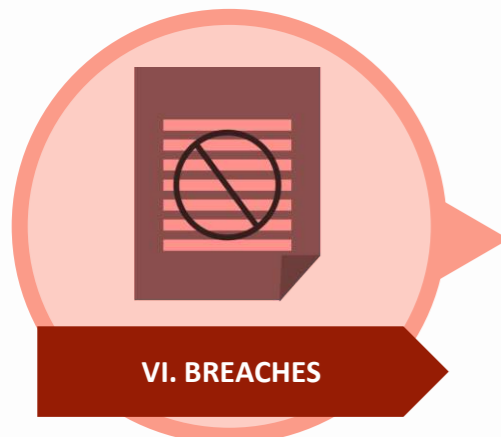
IV. DAY TO DAY

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



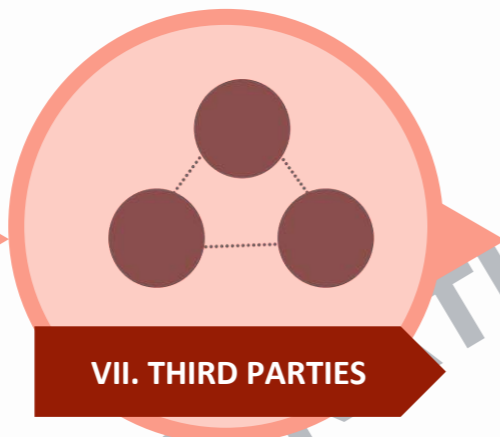
V. DATA SECURITY

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



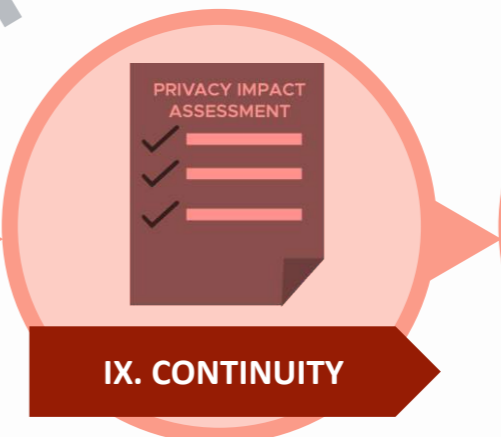
VII. THIRD PARTIES

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



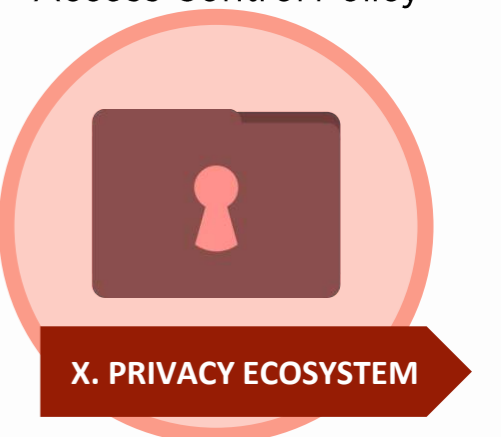
VIII. MANAGE HR

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

ON

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



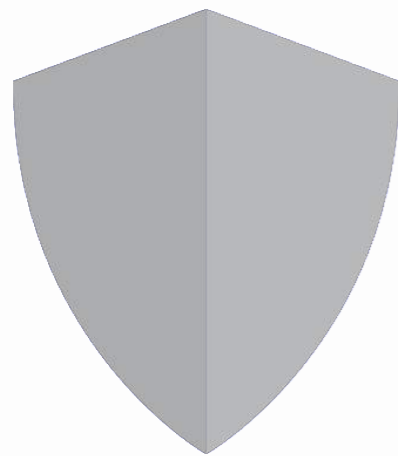
1. Can we feel a culture of **Privacy**?
2. Do you have a **sensible data privacy program**?
3. Is it based on **risk assessment**?
4. Do you **train your staff in data privacy** and protection?
5. Are you prepared for **breach**?



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.





PRIVACY.GOV.PH

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

PROPERTY OF NATIONAL PRIVACY COMMISSION

