What every Government Agency should know.

April 6, 2017 at 3:00 p.m
Crown Legacy Hotel, Baguio City

Raymund Enriquez Liboro
Privacy Commissioner and Chairman

NATIONAL PRIVACY COMMISSION

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

WHAT'S IN IT FOR YOU?

What the **law** is all about

How it will affect **you** and your organization

NATIONAL PRIVACY COMMISSION

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

PARTNER CONTENT JORIS TOONDERS, YONEGO

DATA IS THE NEW OIL OF THE DIGITAL ECONOMY

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

NATIONAL PRIVACY COMMISSION

GMA NEWS ONLINE
YOUR NEWS AUTHORITY

NEWS

Filtered By: News

1004

30

2

0

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.

[redacted] 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, [redacted] remembered posting a photo of his Professional Regulation Commission (PRC) ID online.

"Wala naman akong ginagawang masama," he added.

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

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

55M at risk in 'Comeleak'

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

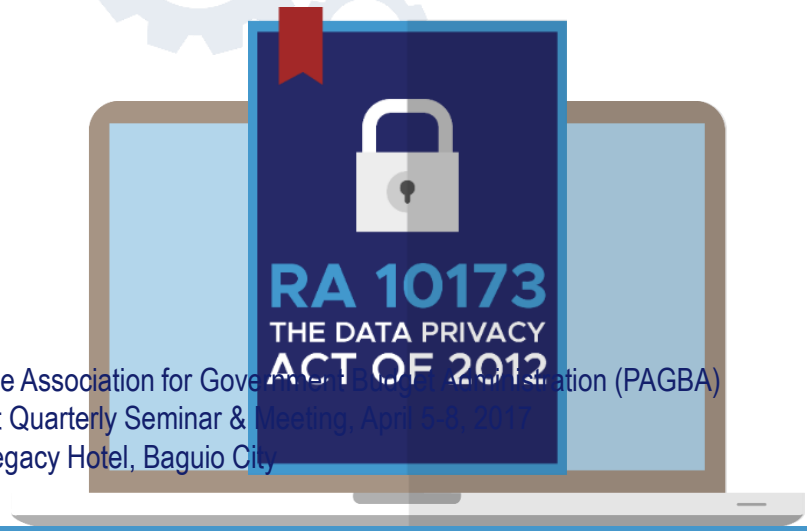
DECEPTIVE CALM The Comelec office at Palacio del Gobernador in Intramuros, Manila, after office hours. The Comelec says the hacking of its website will not compromise the integrity of national elections on May 9.
EDWIN BACASMAS

INTRODUCTION: RA 10173

NATIONAL PRIVACY COMMISSION

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

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.



NATIONAL PRIVACY COMMISSION

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

WHERE IS PRIVACY IN ALL THIS?

NATIONAL PRIVACY COMMISSION

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

The law upholds the right to privacy by **protecting** individual personal information.

NATIONAL PRIVACY COMMISSION

The National Privacy Commission protects individual personal information and upholds the **right to information privacy** by regulating the processing of personal information.

NATIONAL PRIVACY COMMISSION

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

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

NATIONAL PRIVACY COMMISSION

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.

NATIONAL PRIVACY COMMISSION

SALIENT PROVISIONS OF THE DPA

1

Created the National Privacy Commission to monitor the implementation of this law. **SEC. 7**

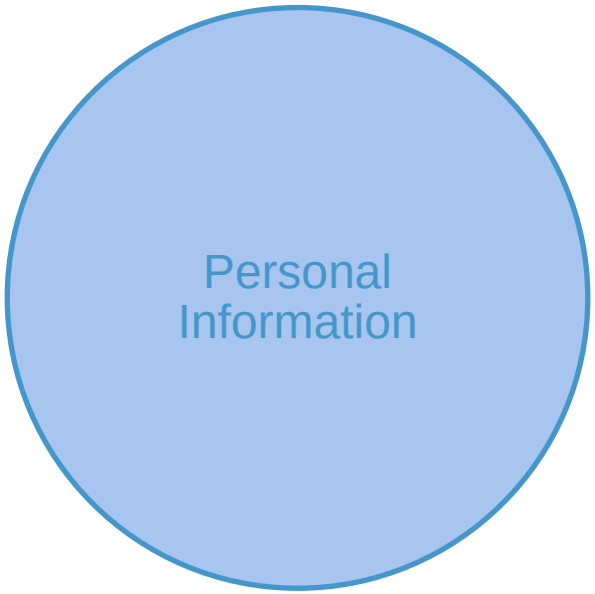
Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

2

It applies to the processing of personal information **SEC. 3 (g)** and sensitive personal information **SEC. 3 (L)**

NATIONAL PRIVACY COMMISSION

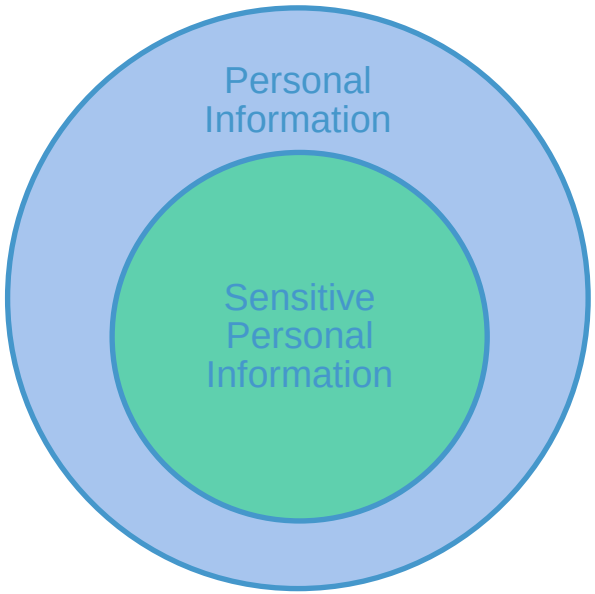
Key concepts



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.

– RA. 10173, Section 3.g

Key concepts



Sensitive personal information refers to personal information:
(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
(3) 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
(4) Specifically established by an executive order or an act of Congress to be kept classified.

– RA. 10173, Section 3.l

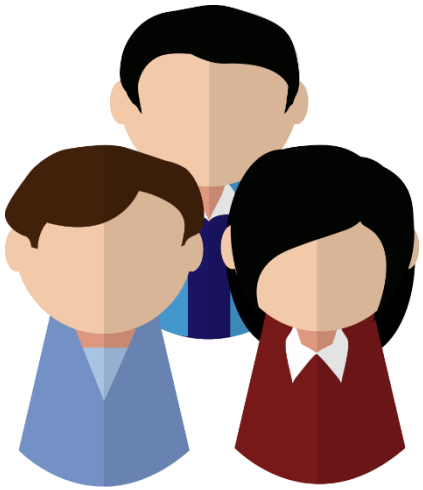
Personal Information	**Sensitive Personal Information** (List based on IRR)	Privileged Information (List based on Rules of Court)
Name	Race	Data received within the context of a protected relationship – husband and wife
Address	Ethnic origin	
Place of work	Marital status	
Telephone number	Age	
Gender	Color	Data received within the context of a protected relationship – attorney and client
Location of an individual at a particular time	Religious affiliation	
	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	
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	Data received within the context of a protected relationship – doctor and patient

3

Data subject has the right to know if their personal information is being processed. The person can demand information such as the source of info, how their personal information is being used, and copy of their information. One has the right to request removal and destruction of one's personal data unless there is a legal obligation that required for it to be kept or processed. **SEC. 15 and 18**

NATIONAL PRIVACY COMMISSION

3. DATA SUBJECT



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

NATIONAL PRIVACY COMMISSION

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

4

Companies who subcontract processing of personal information to third party shall have full liability and can't pass the accountability of such responsibility.

SEC. 14

NATIONAL PRIVACY COMMISSION

5

If the data subject has already passed away or became incapacitated (for one reason or another), their legal assignee or lawful heirs may invoke their data privacy rights. **SEC. 17**

NATIONAL PRIVACY COMMISSION

6

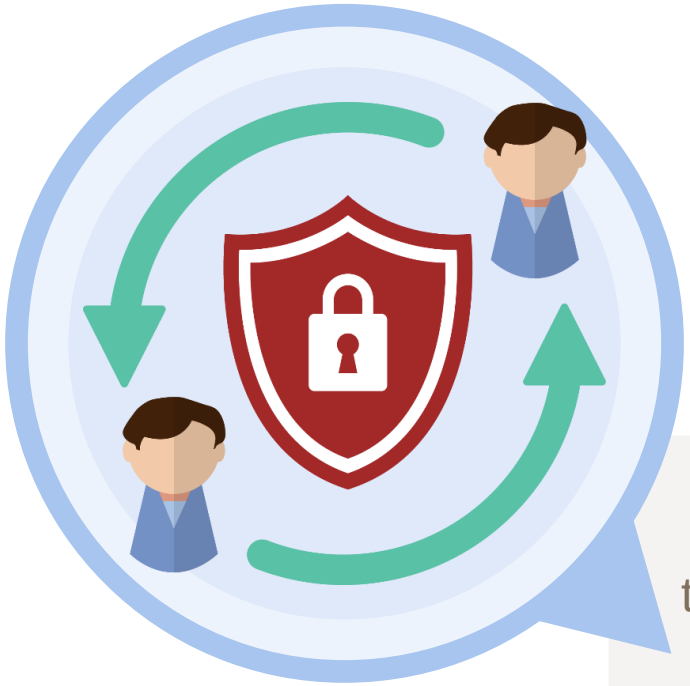
For public officers (working in government), an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall be applied. **SEC. 36**

NATIONAL PRIVACY COMMISSION

7

In case a personal information controller systems or data that got compromised, they must notify the affected data subjects and the National Privacy Commission. **SEC. 20**

NATIONAL PRIVACY COMMISSION



8

Heads of government agencies must ensure their system compliance to this law (including security requirement). Personnel can only access sensitive personal information offsite, limited to 1000 records, in government systems with proper authority and in a secured manner. **SEC. 22**

NATIONAL PRIVACY COMMISSION

10

Provided penalties (up to 5 million as per **SEC. 33**) on the processing of personal information and sensitive personal information based on the following acts:
If at least 100 persons are harmed, the maximum penalty shall apply (**SEC. 35**)

1. **SEC. 25** Unauthorized Processing
2. **SEC. 26** Negligence
3. **SEC. 27** Improper Disposal
4. **SEC. 28** Unauthorized Purposes
5. **SEC. 29** Unauthorized Access
6. **SEC. 30** Concealment of Security Breaches
7. **SEC. 31 and 32** Malicious and Unauthorized Disclosure

NATIONAL PRIVACY COMMISSION

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

Punishable Act	Jail Term	Fine (Pesos)
Unauthorized processing	1y to 3y □ 3y to 6y	500k to 4m
Access due to negligence	1y to 3y □ 3y to 6y	500k to 4m
Improper disposal	6m to 2y □ 3y to 6y	100k to 1m
Unauthorized purposes	18m to 5y □ 2y to 7y	500k to 2m
Intentional breach	1y to 3y	500k to 2m
Concealing breach	18m to 5y	500k to 1m
Malicious disclosure	18m to 5y	500k to 1m
Unauthorized disclosure	1y to 3y □ 3y to 5y	500k to 2m
Combination of acts	3y to 6y	1m to 5m

11

For public officers (working in government), an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall be applied. **SEC. 36**

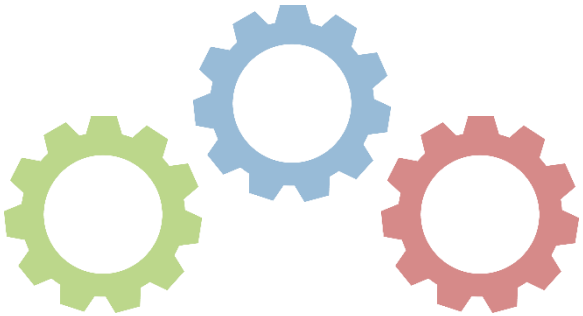
NATIONAL PRIVACY COMMISSION

MORE KEY CONCEPTS

NATIONAL PRIVACY COMMISSION

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

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.

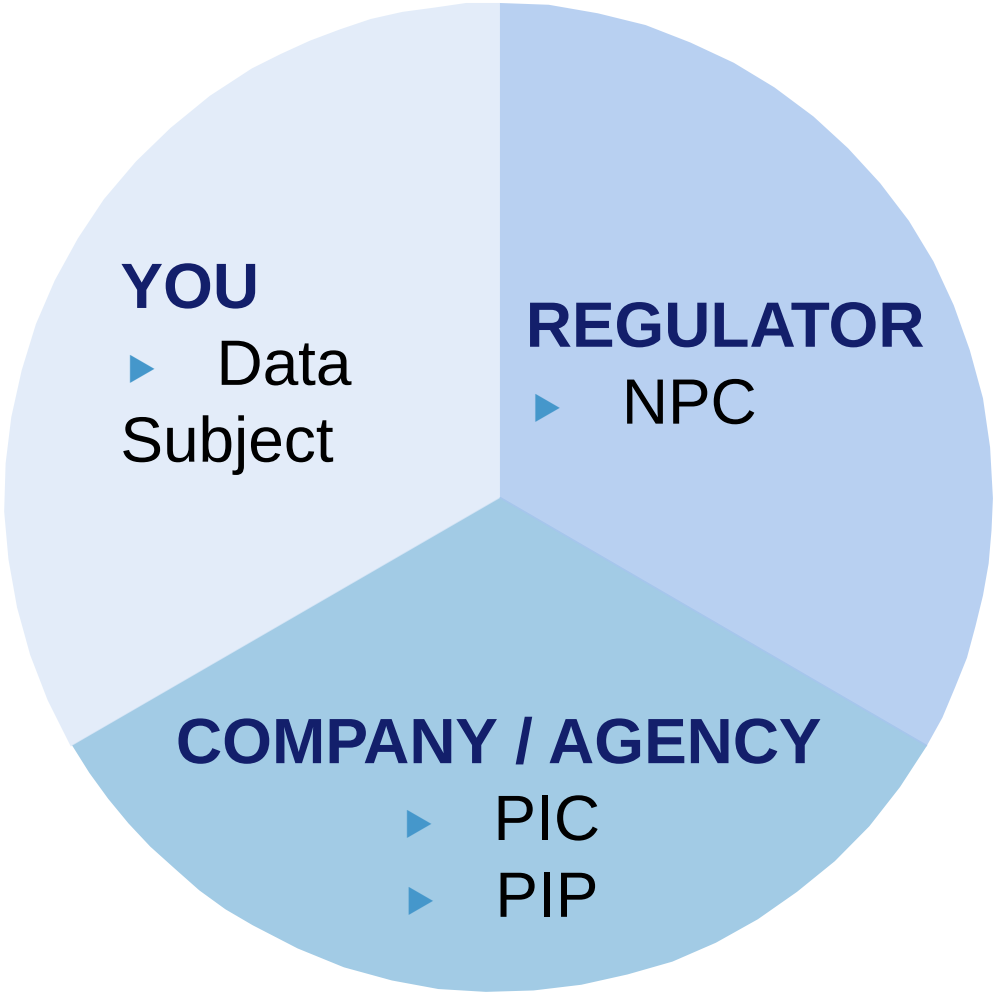
NATIONAL PRIVACY COMMISSION

PROCESSING OF PERSONAL INFORMATION

- **SEC. 12. Criteria for Lawful Processing of Personal Informaiton– The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least of one of the following conditions exists:**

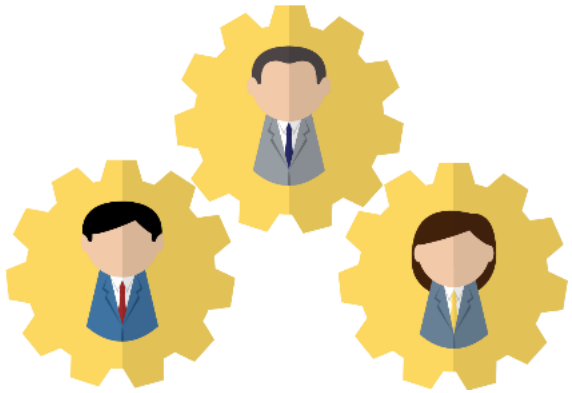
- **(e) The processing is necessary in order to respond to national emergency, to comply with the requirement of public order and safety, and to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate;**

NATIONAL PRIVACY COMMISSION



NATIONAL PRIVACY COMMISSION

Provisions Specific to Government



CHAPTER VII
SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT

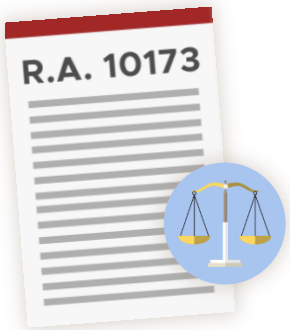
Sec. 22 Responsibility of Head of Agencies.
Sec. 23 requirements Relating to Access by Agency Personnel to Sensitive Personal Information-

a) Onsite and online access
b) Off-site Access

Sec. 24 Applicability to Gov't Contractors

NATIONAL PRIVACY COMMISSION

Why should you comply?



- **Sec. 22.** The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein…

- **Sec. 34.** Extent of Liability. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.

NATIONAL PRIVACY COMMISSION

In the event of a data breach, we will not ask you how many millions you've spent on your hardware and IT experts.

We will, instead, ask whether you've implemented **NPC's five data privacy guidelines**.

PRIVACY COMMISSIONER AND CHAIRMAN RAYMUND E. LIBORO

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

Five Easy Acronyms

NATIONAL PRIVACY COMMISSION

DPO: Data Protection Officer

PIA: Privacy Impact Assessment

PDP: Privacy and Data Protection

BRP: Breach Reporting Procedure

PMP: Privacy Management Program

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

DPO Budget

- The Government Agency needs to allocate a budget to support the implementation of the programs and its sustainability.
- The amount to be allocated would depend on the scope of activities for implementation by the agency with regard to data privacy.

NATIONAL PRIVACY COMMISSION

Designating a DPO is the first essential step towards compliance. You cannot register your systems with the NPC unless you have a DPO. You cannot report your compliance activities unless you go through your DPO.

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

#1: Appoint a DPO (Data Protection Officer)

Legal Basis: Sec. 21, IRR 50, Circ. 16-01

What compliance looks like

- Notarized appointment or designation of a DPO, filed with the NPC
- Evidence of actions taken on basis of DPO recommendations
- Contact details on website (if any)
- Continuing education program

What negligence looks like

- Lack of interaction between DPO and top management, between DPO and functional units
- Inaction on complaints from data subjects
- Non-reporting to NPC

NATIONAL PRIVACY COMMISSION

What DPO will deliver, by when, and how

- **Privacy impact assessments (PIAs)**
  within 30 days months
- **Privacy management program (PMP)**
  within 30 days months, with inputs from top management
- **Privacy and Data Protection (PDP) measures**
  within 60 days
- **Breach reporting procedure (BRP)**
  Be the point of contact or "privacy champion"
- **Be the point of contact for external parties**
- **Notification to NPC within 72 hours**
  in the event of a personal data breach

NATIONAL PRIVACY COMMISSION

What support is needed from the rest of the org'n?

From Process Owners

- Process owners to own/maintain their respective Privacy Impact Assessments
- Process owners to consult on strategic projects involving the use of personal data ("Privacy by Design")
- Breach Drill to be conducted regularly test each Privacy Impact at least once a year

NATIONAL PRIVACY COMMISSION

What support is needed from the rest of the org'n?

From HR

- Roll-out training on privacy and data protection
- Issue security clearances to staff processing personal data (such clearance to be made contingent on passing the privacy training). DPOs must have access to all security clearances issued.
- Implement the recommended organizational controls

NATIONAL PRIVACY COMMISSION

What support is needed from the rest of the org'n?

From Other Support Teams

- IT to implement the recommended technical controls
- Security to implement the recommended physical controls
- Internal audit to test internally for compliance

NATIONAL PRIVACY COMMISSION

What support is needed from the rest of the org'n?

From Top Management

- Budget support for security controls (technical, organizational, physical), for compliance tools and technology, for informational and training activities, for consultants, external auditors, advisors
- Incorporating compliance into the performance bonus parameters of those concerned, especially for those handling personal data
- Drive the message throughout the organization
- Drive the urgency (e.g. like the SARS epidemic, when everyone started installing hand sanitizers)

NATIONAL PRIVACY COMMISSION

#2: Data Processing adheres to Transparency, Legitimate Purpose, and Proportionality

Legal Basis: Sec. 11-15, IRR 21-23 and 43-45, Circ. 16-01 and 16-02

What compliance looks like

- Privacy policies cascaded throughout the organization and updated as needed
- Data handlers have security clearance and privacy training
- Privacy notice where appropriate, e.g. on website
- Data sharing agreements in place
- Privacy impact assessments conducted and up-to-date
- Service providers in compliance

What negligence looks like

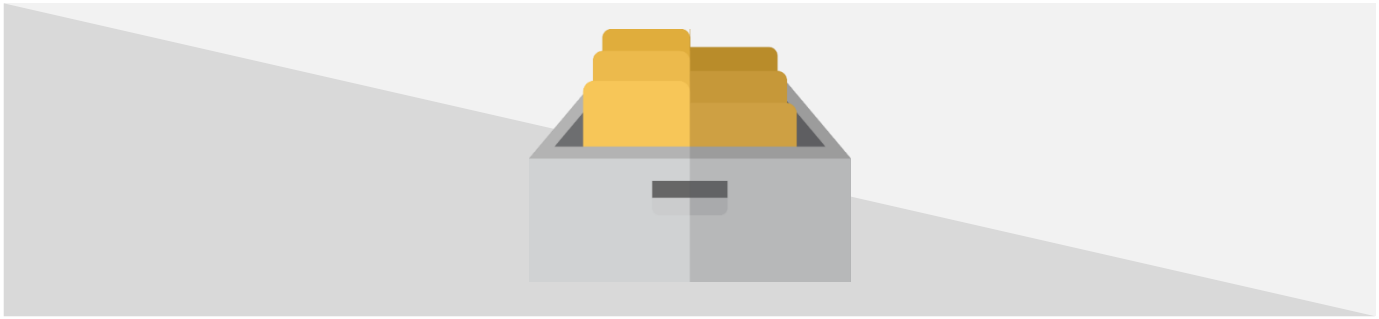
- Privacy policy sits on shelf
- No security clearance or privacy training for data handlers
- No privacy notice when collecting personal data
- Overcollection
- Data sharing without agreements
- No privacy impact assessments
- No compliance obligations for service providers

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.

#3: Maintain Privacy and Protection of Data

Legal Basis: Sec. 20.a-e, Sec. 22 an d 24, IRR 25-29, Circ. 16-01

What compliance looks like

- Data protection risks identified, and the appropriate up-to-date controls are in place to manage these risks
- Data protection policies cascaded throughout the org'n and updated as needed
- Frequent monitoring and vulnerability scanning
- Regular security and business continuity drills are conducted
- Service providers in compliance

What negligence looks like

- Generic controls in place
- Controls not updated for new risks/threats
- Controls are not complied with
- Lax cyber-hygiene practices
- No compliance obligations for service providers
- No periodic drills or monitoring
- No venue for data subjects to access or correct/rectify their own data

NATIONAL PRIVACY COMMISSION

RA 10173, Sec. 23 (b) Off-site Access – Unless otherwise provided in guidelines to be issued by the Commission, sensitive pe
tra
un
an

Circular 16-01.

SECTION 10. When a government agency engages a service provider for the purpose of storing personal data under the agency's control or custody, the service provider shall function as a personal information processor and comply with all the requirements of the Act, its IRR and all applicable issuances by the Commission.

SECTION 12. The Commission recommends ISO/IEC 27018 as the most appropriate certification for the service or function provided by a service provider under this Rule.

Circular 16-01, Sections 7 to 13 Storage of Personal Data

"Owned" Data Center

- Covered as PIC
- Subject to NPC Audit (Sec. 11)
- AES-256 Encrypted (Sec. 8)
- Access control system (Sec. 9)
- Archives are also covered (Sec. 13)

"Non-owned" Data Center

- Covered as PIP (sec. 10)
- Subject to NPC Audit (Sec. 11)
- ISO 27018 (Sec. 12)
- AES-256 Encrypted (Sec. 8)
- Archives are also covered (Sec. 13)
- Contract subject to review (Sec. 7)
- If data is stored outside the country, geographic location must be specified in contract (IRR, Sec. 44.a)

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

THE DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK

I. GOVERNANCE

1. Choose a DPO

II. BASELINE

2. Conduct PIA
3. Register

III. ORGANIZATION

4. Privacy Policy
5. Framework

IV. DAY TO DAY

6. Privacy Notice
7. DS Rights
8. Retention
9. Disposal

V. MANAGE HR

10. Training
11. Disposal

VI. DATA SECURITY

12. Data Center
13. Encryption
14. Access Policy
15. Transfers

VII. THIRD PARTIES

16. Compliance
17. Agreements
18. Due Diligence
19. Notification
20. Access Policy

VIII. BREACHES

21. Assessment
22. Monitoring
23. Team
24. Continuity
25. Review
26. Notification

IX. PROJECTS

27. Conduct PIA

X. MANAGE LEGAL

28. Monitor
29. Contracts
30. Due Diligence
31. Advisory

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City

#4: Report Breach within 72 hours

Legal Basis: Sec. 20.f and 30, IRR 38-42 and 57, Circ. 16-03

What compliance looks like

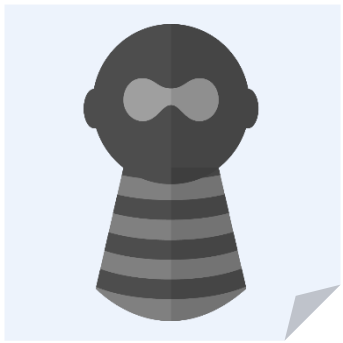
- Formation of a data breach response team with clearly defined roles and responsibilities
- Clearly defined and up-to-date incident response procedure that covers assessment, mitigation, notification and recovery actions
- Regular breach drills are conducted
- Service providers in compliance

What negligence looks like

- No response team or procedures
- No drills
- No compliance obligations for service providers
- No post-breach reports
- No notification within 72 hours (an act punishable by 18 months to 5 years of imprisonment and and a fine of 500,000 to 1,000,000 pesos)

NATIONAL PRIVACY COMMISSION

CAUSES OF BREACH



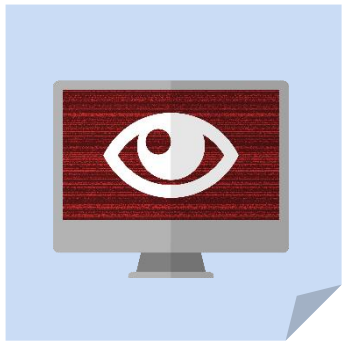
Theft or Break-in

Poor Controls

Equipment Failure

Human Error

Unforeseen Circumstances



Equipment Failure

ACTIONS TO TAKE

NATIONAL PRIVACY COMMISSION

#5: Register with the NPC

Legal Basis: Sec. 24, IRR 33 and 46-49

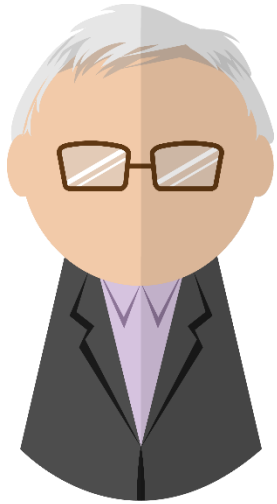
What compliance looks like

- Registration with the NPC is up-to-date and contains all necessary compliance documentation
- Registration includes all automated processing operations that would have legal effect on the data subject
- Annual report summarizing documented security incidents and personal data breaches
- Service providers in compliance

What negligence looks like

- No registration
- Out-of-date registration
- No compliance obligations for service providers

NATIONAL PRIVACY COMMISSION



PRIVACY.GOV.PH

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

NATIONAL PRIVACY COMMISSION

RA 10173
DATA PRIVACY ACT OF 2012

Philippine Association for Government Budget Administration (PAGBA)
2017 1st Quarterly Seminar & Meeting, April 5-8, 2017
Crown legacy Hotel, Baguio City