A Primer on **Compliance** to the Data Privacy Act

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Sec. 21 (b) **The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act.**

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Who is liable? Who goes to jail?

- **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.

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

The Obligations you must comply with

Data Privacy Act of 2012

IRRs (promulgated 2016)

2016 Series

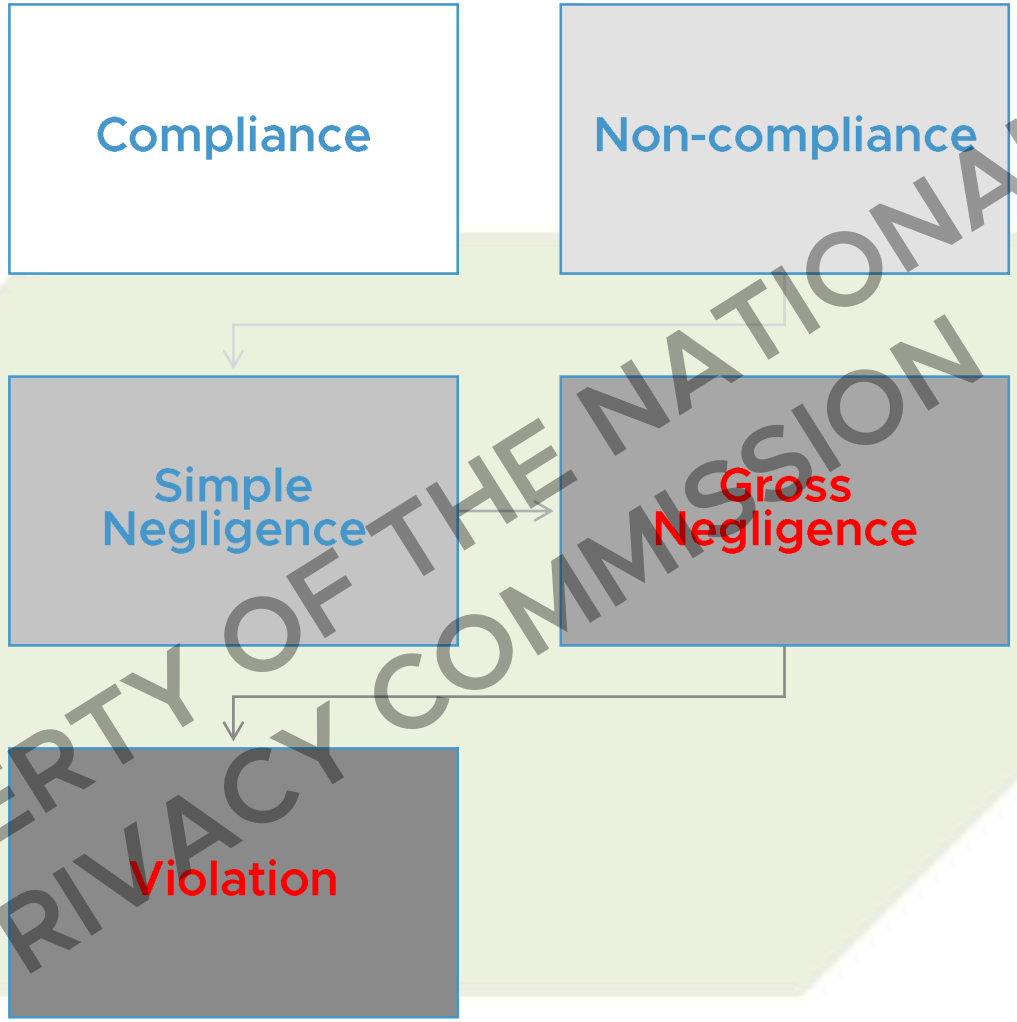
- Circular 16-01 Gov't Agencies
- Circular 16-02 Data Sharing
- Circular 16-03 Breach Mgmt
- Circular 16-04 Rules Procedure

2017 Series

- *Advisory 17-01 DPO Guidelines*
- *Advisory 17-02 PDS Guidelines*
- *Advisory 17-03 PIA Guidelines*
- Circular 17-01 Registration

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION



Republic Act No. 10173

August 15, 2012

SEC. 26. (b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

SEC. 35. Large-Scale. – The maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal information of at least one hundred (100) persons is harmed, affected or involved as the result of the above mentioned actions.

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

PUNISHABLE ACT	JAIL TERM	FINE (PESOS)
Access due to negligence	1y to 3y | 3y to 6y	500k to 4m
Unauthorized processing	1y to 3y | 3y to 6y	500k to 4m
Unauthorized purposes	18m to 5y | 2y to 7y	500k to 2m
Improper disposal	6m to 2y | 3y to 6y	100k to 1m
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

Structure of RA 10173, the Data Privacy Act

Sections 1-6. Definitions and General Provisions

Sections 7-10. National Privacy Commission

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

Section 22-24. Provisions Specific to Government

Section 25-37. Penalties

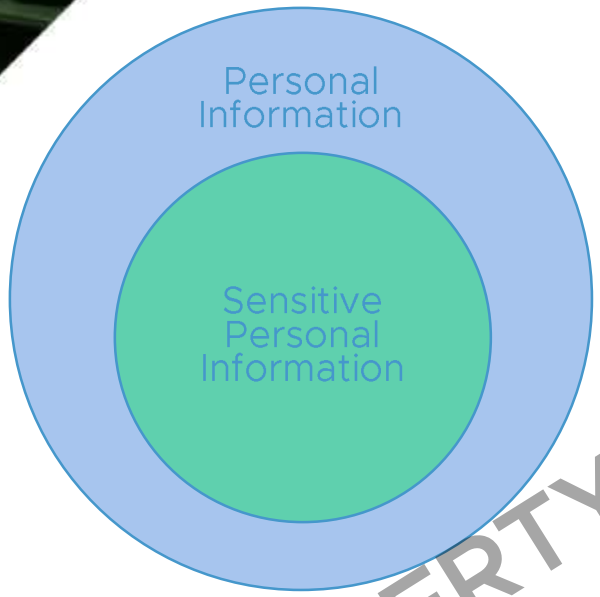
DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Definitions, Sec. 3

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*

Definitions, Sec. 3



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*

1.) **University of Maryland**

In March 2014, more than 300,000 student, faculty and staff records were compromised at University of Maryland. Though no financial, medical or academic records were compromised, the breach did include names, birth dates, university ID numbers and even Social Security numbers. According to University of Maryland's student newspaper, *The Diamondback*,"The database that was accessed contained information from everyone who has received a university ID from the College Park or Shady Grove campuses since 1998."

2.) **North Dakota University**

In February, 2014, a server at the North Dakota University System storing personal information of nearly 300,000 past and present students was hacked. Such personal information included names and social security numbers.

3.) **Butler University**

The third largest data breach in 2014 among colleges happened at Butler University. According to the University Herald, hackers got access to the school's network, exposing personal information of nearly 200,000 people. Personal information exposed included names, birth dates, driver's licenses, social security numbers, and bank account information.

Data from data-breach.silk.co

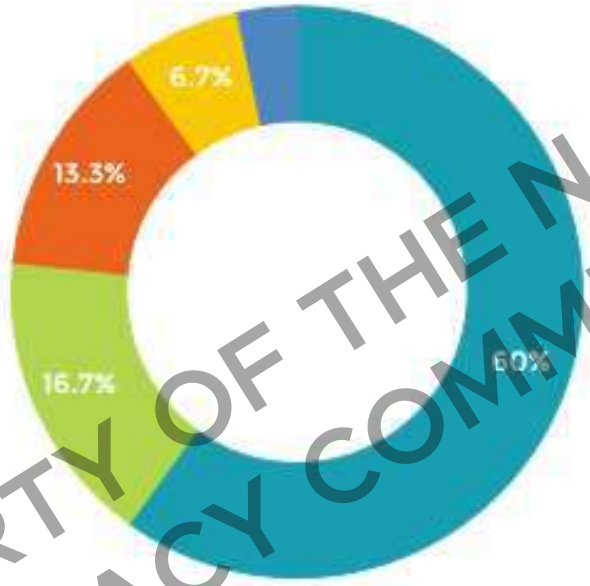
DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Type of Target: Educational Institutions

Filter by Type of Breach

Filter by Title



Type of Breach

- Hacking or malware
- Unintended disclosure
- Portable device
- Insider
- Unknown or other

Data from data-breach.silk.co

Definition of PIC vs PIP

PIC

"Personal Information Controllers" those who decide what data is collected and how it is processed (example: Bank X, Hospital Y).

PIP

"Personal Information Processors" those who process data as instructed by the controllers (example: shared services, IT vendor, external lab).

Sabre Breach May Have Exposed Payment Data at 36,000 Hotels

By Jeff Goldman, Posted May 4, 2017

The company recently identified unauthorized access to payment information processed through its SynXis Central Reservation system.

The travel technology company Sabre Corp. has acknowledged that its hotel reservation system was recently breached, according to investigative reporter Brian Krebs.

The breach affects a platform that Sabre says is used by more than 36,000 hotels worldwide.

In its most recent quarterly filing with the SEC, the company stated, "We are investigating an incident involving unauthorized access to payment information contained in a subset of hotel reservations processed through the Sabre Hospitality Solutions SynXis Central Reservation system."

PICs vs. PIPs

- The agency or corporation who controls the processing of personal data, the one who decides
- There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing
- Not the employee, not the DPO, not the CIO

- Individual, Corporation or other body who processes the personal data for a Personal Information Controller
- Personal information processor should not make use of personal data for its own purpose
- Employees of the PIC are not considered PIPs

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
☐ Notarized designation of a DPO/COP, filed with the NPC ☐ Evidence that DPO/COP recommendations are taken into consideration when making decisions ☐ Contact details are easy to find (e.g. on website) ☐ Continuing education program for the DPO/COP	☐ No DPO or COP (in which case CEO or HoA is the default DPO) ☐ Lack of interaction between DPO/COP and top management ☐ Lack of interaction between DPO/COP and functional units ☐ Communication from the DPO/COP is largely ignored ☐ No continuing education program for the DPO/COP

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
☐ Up-to-date organizational inventory of processes that handle personal data, including the list of process owners ☐ PIAs have been conducted, and are owned and kept up-to-date by the process owner ☐ Stakeholders (those involved in the information life cycle) have been consulted as part of the PIA process ☐ PIA includes a privacy risk map, a list of controls, an implementation plan, and a monitoring/evaluation milestone	☐ No PIAs ☐ Process owners do not "own" the PIAs ☐ PIAs are not updated when changes are made to the process, or to the technologies being used in the process ☐ Stakeholders are not consulted for the PIA ☐ Controls identified during the PIA are not implemented

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

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

Legal Basis: 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
☐ Notarized designation of a DPO/COP, filed with the NPC ☐ Evidence that DPO/COP recommendations are taken into consideration when making decisions ☐ Contact details are easy to find (e.g. on website) ☐ Continuing education program for the DPO/COP	☐ No DPO or COP (in which case CEO or HoA is the default DPO) ☐ Lack of interaction between DPO/COP and top management ☐ Lack of interaction between DPO/COP and functional units ☐ Communication from the DPO/COP is largely ignored ☐ No continuing education program for the DPO/COP

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

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

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

Appoint an individual accountable for compliance
☐ Notarized designation of a DPO/COP, filed with the NPC
☐ Evidence that DPO/COP recommendations are taken into consideration when making decisions
☐ Contact details are easy to find (e.g. on website)
☐ Continuing education program for the DPO/COP

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

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

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

Ineffective data protection governance
☐ No DPO or COP (in which case CEO or HoA is the default DPO)
☐ Lack of interaction between DPO/COP and top management
☐ Lack of interaction between DPO/COP and functional units
☐ Communication from the DPO/COP is largely ignored
☐ No continuing education program for the DPO/COP

Selecting a DPO

Minimum requirements

- business expertise
- knowledge of privacy principles
- empowered to be a change agent

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

CIPP

The "what"
Laws and regulations

The CIPP shows that you understand the laws, regulations and standards of privacy in your jurisdiction or discipline.

CIPM

The "how"
Operations

The CIPM says that you understand how to use process and technology to manage privacy in an organization—regardless of the industry or jurisdiction.

CIPT

The "how"
Technology

The CIPT shows that your know how to manage and build privacy requirements and controls into technology.

Selecting a DPO

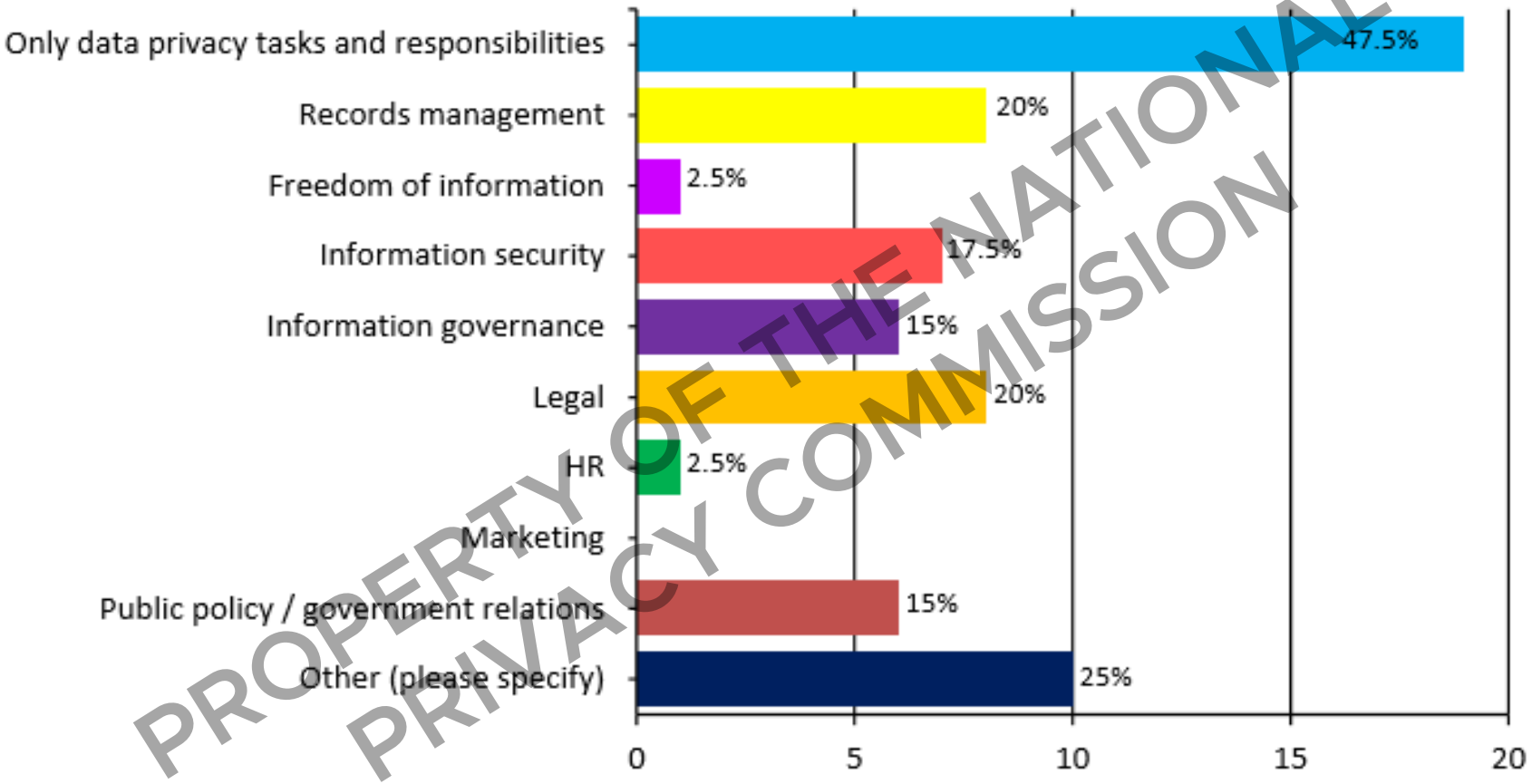
Minimum requirements

- business expertise
- knowledge of privacy principles
- empowered to be a change agent

Options

- full-time or part-time (1 or 2)
- supported by a team or a committee
- full-blown task force or data protection office

What other (non-data privacy) roles and responsibilities does the DPO/CPO have in your organisation?



DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Selecting a DPO

Minimum requirements

- business expertise
- knowledge of privacy principles
- empowered to be a change agent

Options

- full-time or part-time (1 or 2)
- supported by a team or a committee
- full-blown task force or data protection office

One size doesn't fit all

- low risk
- medium risk
- high risk

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

	Low	Medium	High
Type of Data	No personal data	Personal information	Sensitive Personal Info
Volume	Less than 250 records	Less than 1,000 records	1,000 or more records
Origin		Filipino citizens only	Includes other nationalities
Access	Limited to Onsite	Onsite as well as Offsite	External Parties
Time of Access	Less than 8 hours	8 to 12 hours	24 hours
Number of Users	Less than 50	Less than 250	250 or more
Response Req't.	None	Sub-minute	Sub-second
Storage Media	Non-digital	All digital	Mixed
Storage Location		One site	Multiple sites
Big Data Projects	No plans	Within 3 years	Currently operating

What does a DPO do?

a. Monitor compliance
b. Ensure conduct of PIAs
c. Ensure data subjects' rights are respected
d. Ensure proper breach management
e. Cultivate internal awareness on data privacy
f. Advocate a privacy-by-design approach
g. Serve as contact person for privacy matters
h. Serve as conduit with the NPC
i. Perform other duties as may be assigned

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

*See NPC Advisory 2017-01, pp. 6-7

Support needed from Process Owners

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")
- Process owners to conduct breach drills on their respective processes

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Support needed from HR Team

HUMAN RESOURCES

- Roll-out training on privacy and data protection
- Issue security clearances to staff processing personal data. DPOs must have access to all security clearances issued.
- Implement the recommended organizational controls

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Support needed from Legal

LEGAL

- Legal to ensure that all PIP/service provider contracts, job orders, etc. are compliant. For example, all PIPs must also have their own DPO
- Legal to ensure that all external sharing of data meets the required guidelines of the NPC

Support needed from Others

OTHERS

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

Support needed from Top Management

TOP MANAGEMENT

- Budget support for security controls 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

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

What a DPO might need to build capacity

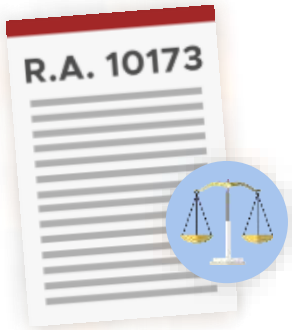
- ✓A support group
- ✓A mentor
- ✓An IT security audit
- ✓Litigation support
- ✓Access to top management
- ✓Continuing education
- ✓Organizational leverage
- ✓Tool support
- ✓Support staff

Summary: Advisory 17-01

- Must be an employee of the PIC or PIP (p. 5), however the functions of a DPO or COP **may be subcontracted or outsourced** to a third-party service provider (p. 8)
- No conflict of interest – cannot also be a data or process owner (p. 6)
- The PIC or PIP **should not directly or indirectly penalize or dismiss** the DPO or COP for performing his or her tasks (p. 8)
- The PIC or PIP **should follow the advice** of the DPO or explain and document why it did not (p. 9)
- COP must be **"supervised"** by a DPO

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

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



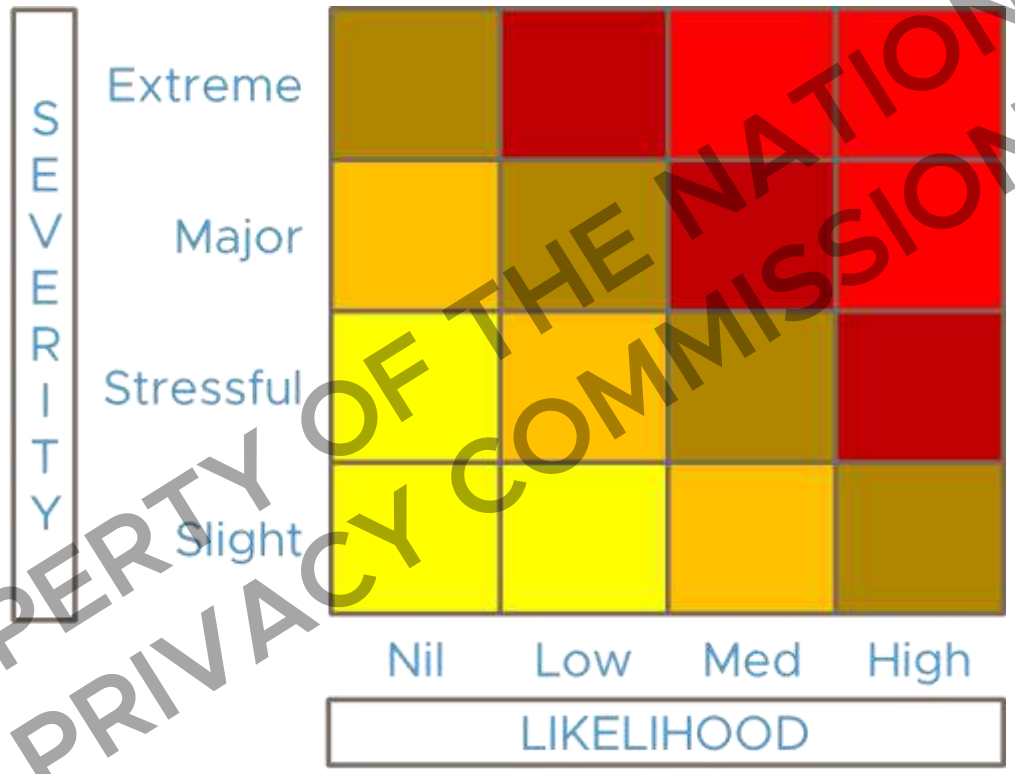
Sec. 20 (c) "The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation."

How will you know what are "the risks represented by the processing"?

DP FOR THE ACADEME 4

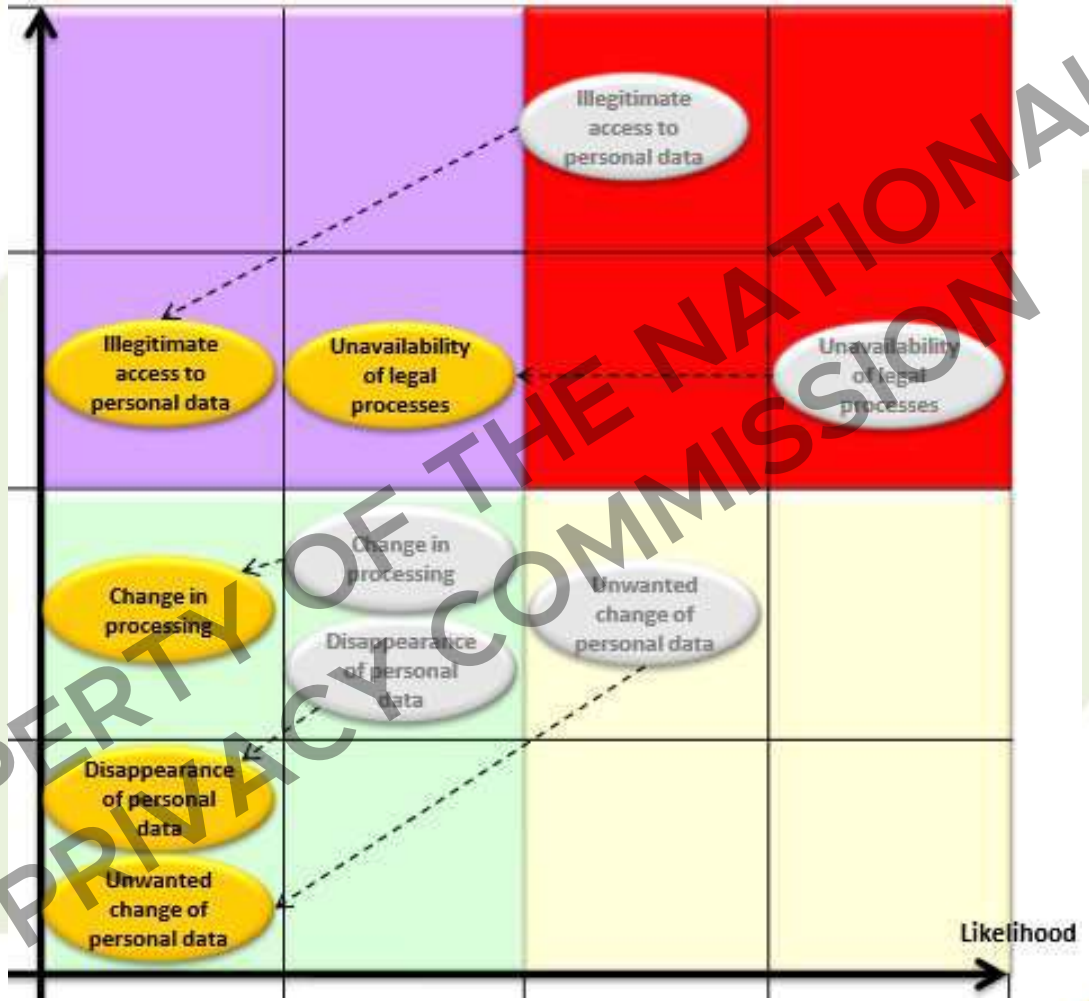
NATIONAL PRIVACY COMMISSION

Privacy Risk Map



DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION



DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

PIA: both process & instrument

ISO/IEC 29134 (2017)

- Overall process of identifying, analyzing, evaluating, consulting, communicating, planning to treat potential privacy impacts
- An instrument for assessing the potential impacts on privacy of a process, information system, program, software module, device or other initiative which processes PII
- Framed within an org's broader risk management framework
- An instrument for taking actions as necessary in order to treat privacy risk, in consultation with stakeholders.

PIA Process

Organization-wide

1. Make an inventory of personal data held by the company/agency (including location and type of media)
2. Identify the projects, processes, programs, or measures that act on this data
3. Regularly review the list to determine whether a new/revised PIA is necessary

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

PIA Process (2)

Planning and Mobilization

- Setup the team, finalize the scope
- Determine what resources are needed
- Identify stakeholders and establish consultation plan

Perform the Assessment

- Consult stakeholders, analyze risks, create risk map
- Determine necessary controls/measures
- Create risk management plan, get sign off

Implement the control framework

- Deploy risk management controls
- Monitor and evaluate on a regular basis

PIA Components

- Ownership
- Stakeholder Involvement
- Privacy Risk Map
- Controls/Measures Framework
- Sign-off
- Implementation / Monitoring Plan

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

Legal Basis: 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
☐ Up-to-date organizational inventory of processes that handle personal data, including the list of process owners ☐ PIAs have been conducted, and are owned and kept up-to-date by the process owner ☐ Stakeholders (those involved in the information life cycle) have been consulted as part of the PIA process ☐ PIA includes a privacy risk map, a list of controls, an implementation plan, and a monitoring/evaluation milestone	☐ No PIAs ☐ Process owners do not "own" the PIAs ☐ PIAs are not updated when changes are made to the process, or to the technologies being used in the process ☐ Stakeholders are not consulted for the PIA ☐ Controls identified during the PIA are not implemented

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

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

Legal Basis: 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
☐ Up-to-date organizational inventory of processes that handle personal data, including the list of process owners ☐ PIAs have been conducted, and are owned and kept up-to-date by the process owner ☐ Stakeholders (those involved in the information life cycle) have been consulted as part of the PIA process ☐ PIA includes a privacy risk map, a list of controls, an implementation plan, and a monitoring/evaluation milestone

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

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

Data processing controls do not take into account the risks to the rights and freedoms of data subjects
☐ No PIAs ☐ Process owners do not "own" the PIAs ☐ PIAs are not updated when changes are made to the process, or to the technologies being used in the process ☐ Stakeholders are not consulted for the PIA ☐ Controls identified during the PIA are not implemented

Pillar 3: Write Your Plan: Create Your Privacy Management Program

Legal Basis: Sec. 11-15 of the DPA, Sections 21-23 and 43-45 of the IRR, Circulars 16-01 and 16-02

Processing of data is according to privacy principles of transparency, legitimate purpose, and proportionality	Data processing not according to privacy principles of transparency, legitimate purpose, and proportionality
☐ Personal data is processed as per Sections 12 and 13 of the DPA ☐ Privacy principles are embedded into HR, Marketing, Operations, Security, and IT policies, are cascaded throughout the organization, and are updated as needed ☐ Data handlers have security clearance and privacy training ☐ Privacy notices are posted where appropriate (e.g. on website) ☐ Data sharing agreements are in place ☐ Tools in place to monitor compliance of the organization ☐ Records of data processing are maintained	☐ Processing fails to meet the criteria for lawful processing of personal data ☐ No privacy policy ☐ Privacy policy exists, but is not cascaded throughout the organization ☐ No privacy training or security clearance for data handlers ☐ Data is being shared without data sharing agreements ☐ No records of data processing

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Data Privacy Principles

"Transparency" – no surprises in how the data collected is being processed

"Legitimate purpose" – required by law and not contrary to public morals

"Proportionality" – collect only what's needed and commensurate to the benefits

DP FOR THE ACADEME 4

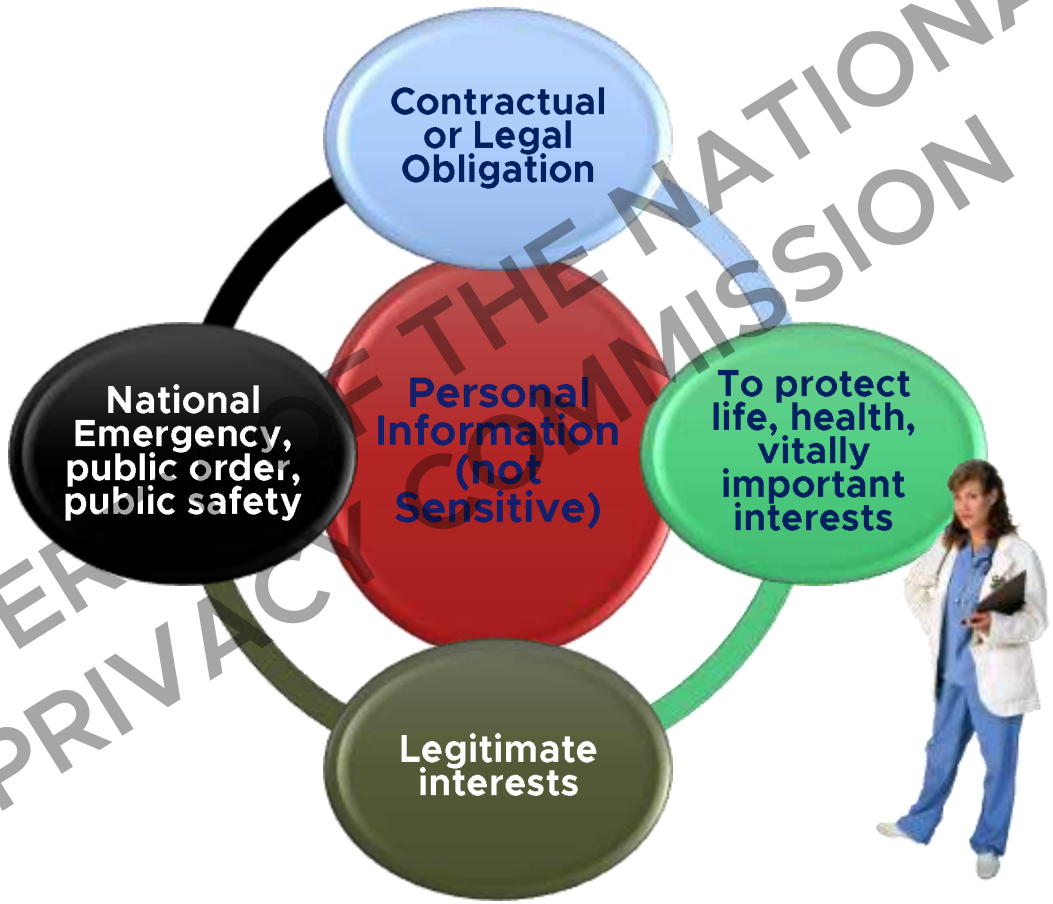
NATIONAL PRIVACY COMMISSION

Be sure to read...

Section 12 – Conditions under which processing Personal Information is ALLOWED...

Section 13 – Processing of Sensitive Personal Information is PROHIBITED except in the following cases...

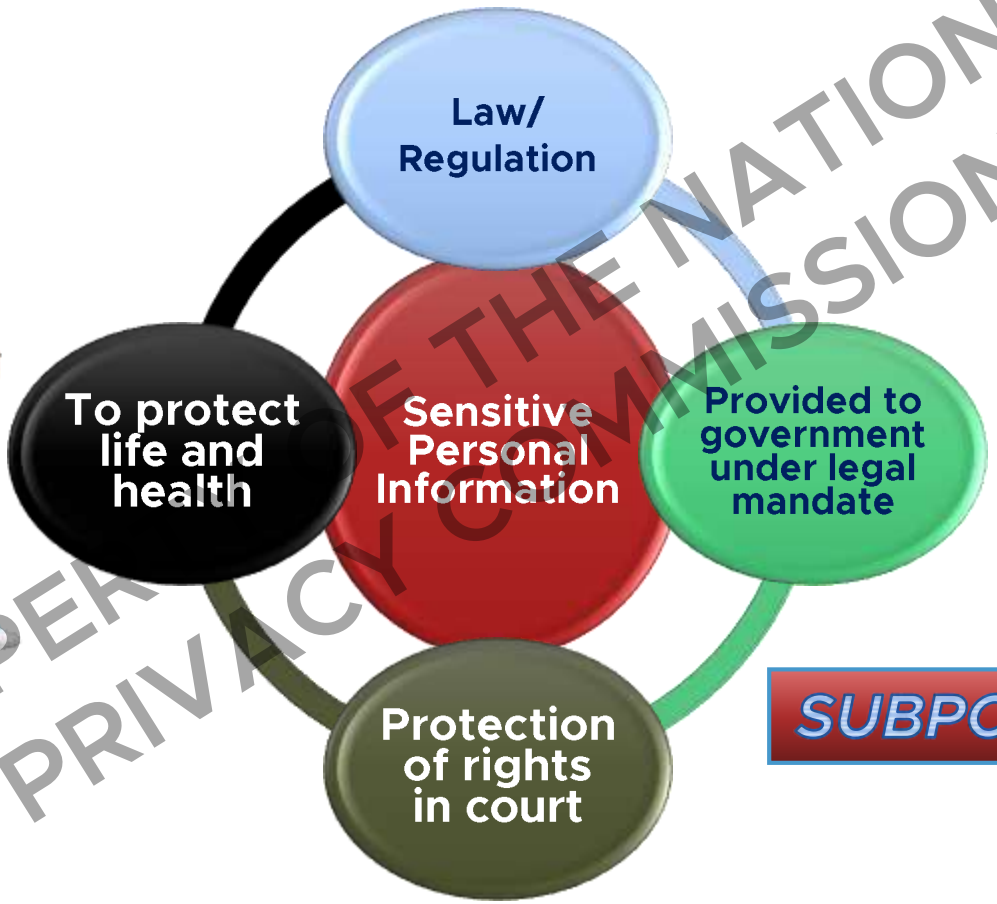
Section 12



DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Section 13



SUBPOENA

When it comes to consent

If It's NOT CLEAR It's NOT Consent

Do you share data?

Are you providing ACCESS to personal data you have collected to a third party, e.g. PRC?

Is there a specific provision of LAW that specifically requires data sharing? (Ex. Reporting under R.A. No. 9510 – CISA)

If there is no specific provision of law, is there a public service and a STATUTORY MANDATE? Do you have CONSENT of the data subject?

What's in a DSA?

- Purpose of Data Sharing, including the Public Function and Public Service it facilitates
- Parties to the agreement (usually 2 or more PICs)
- Term or Duration of the Agreement
- Overview of operational details and general description of security measures
- How data subjects can exercise their rights

Pillar 4: Be Accountable: Implement your Privacy & Data Protection (PDP) Measures

- SEC. 20 (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

- Guard against: Destruction, Alteration, Disclosure
- Objective/Goal: Availability, Integrity, Confidentiality (CIA)

- Measures: Organizational, Physical, Technical

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Pillar 4: Be Accountable: Implement your Privacy & Data Protection (PDP) Measures

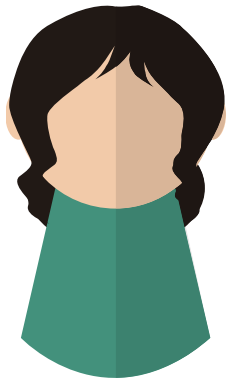
Upholding the rights of data subjects	Neglecting the rights of data subjects
☐ Data subjects are apprised of their rights through a privacy notice ☐ Consent is obtained prior to the collection and processing of data ☐ Data subjects are provided a means to access their data ☐ Data subjects are provided a venue to correct/rectify their data ☐ Data subjects know who to complain to if their rights are violated ☐ Complaints are acted upon quickly (within 30 days) ☐ These rights are upheld when invoked by the lawful heirs or assigns of the data subject	☐ No privacy notice when collecting personal data ☐ Consent is not obtained prior to the collection/processing of data ☐ No venue for data subjects to access their data ☐ No venue for data subjects to correct/rectify their data ☐ No contact details on how to lodge a complaint ☐ Complaints take a long time to be remedied ☐ Inaction on complaints from data subjects ☐ Overcollection of personal data

Maintaining confidentiality, integrity, and availability	Insufficient controls to maintain confidentiality, integrity, and availability
☐ Data protection risks have been identified and documented ☐ Appropriate and up-to-date organizational, physical, and technical controls are in place to manage these risks (e.g ISO:IEC 27002) ☐ Data protection policies are cascaded throughout the organization and updated as needed ☐ Vulnerability scanning is conducted at least once a year ☐ Business continuity drills are conducted at least once a year ☐ For data stored outside the Philippines, location of foreign country is defined ☐ For personal data stored in the cloud, NPC recommends that provider is ISO:IEC 27018 compliant (from Circular 16-01) ☐ For digitized personal data, NPC recommends 256-bit AES for data at rest and in transit (from Circular 16-01)	☐ Controls for data protection are not appropriate for the risks identified ☐ Controls for data protection are not updated for new risks/threats ☐ Controls for data protection are not complied with ☐ Cyber-hygiene practices are lax ☐ Business continuity drill has not been conducted in the last 12 months ☐ Security vulnerability scanning has not been conducted in the last 12 months

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Sec. 16-18
Rights of Data Subjects



- ✓Right to be informed
- ✓Right to object
- ✓Right to access
- ✓Right to correct/rectify
- ✓Right to block/remove
- ✓Right to data portability
- ✓Right to file a complaint
- ✓Right to be indemnified

The NPC recommends the following data protection standards for government agencies:

ISO:IEC 27001/27002

- As the standard to assess control gaps in data protection framework
- Ref: Section 6, NPC Circular 16-01

ISO:IEC 27018

- As the most appropriate certification for a cloud service provider
- Ref: Section 12, NPC Circular 16-01

AES 256

- As the standard for encrypting personal data, at rest and in transit
- Ref: Section 8, NPC Circular 16-01

Multi-factor authentication

- As the standard for allowing online access to personal data
- Ref: Section 18, NPC Circular 16-01

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Pillar 5: Be Prepared: Regularly exercise your Breach Reporting Procedures

Legal Basis: Sec. 20.f and 30 of the DPA, Sections 38-42 and 57 of the IRR, Circular 16-03

IRR Sec. 38 (a) The Commission and affected data subjects shall be notified by the PIC within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred.

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Pillar 5: Be Prepared: Regularly exercise your Breach Reporting Procedures

Legal Basis: Sec. 20.f and 30 of the DPA, Sections 38-42 and 57 of the IRR, Circular 16-03

Able to report breach within 72 hours	Unable/unwilling to report breach within 72 hours
☐ Formation of a data breach response team with clearly defined roles and responsibilities ☐ Clearly defined and up-to-date incident response procedure ☐ Breach drills are conducted at least once a year	☐ No breach response team ☐ No breach response policy or procedures ☐ Breach drill has not been conducted in the last 12 months ☐ No notification of the NPC within 72 hours of discovery of a breach of personal data (possible criminal offense)

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Pillar 6: Registration

Legal Basis: Appendix 1 of Circular 17-01

Who should register? UNIVERSITIES, COLLEGES AND OTHER INSTITUTIONS OF HIGHER LEARNING, ALL OTHER SCHOOLS AND TRAINING INSTITUTIONS

Sec. 24 of the DPA, and Sections 33 and 46-49 of the IRR, Circular 17-01

Register with the NPC	Non-registration with the NPC
☐ Registration with the NPC is up-to-date and contains all necessary compliance documentation ☐ Registration of all automated processing operations that have legal effect on the data subject ☐ Annual report summarizing documented security incidents and personal data breaches ☐ Service providers are also registered	☐ No registration (must be renewed annually) ☐ Out-of-date registration (must be updated within two months of any change) ☐ Non-reporting to NPC of documented security incidents and personal data breaches

Sec. 14 of the DPA, Sections 43-45 of the IRR, Circular 17-01

Service providers agree to honor their compliance obligations	Service providers in default of their compliance obligations
☐ All service providers are contractually bound to comply with the DPA, the IRR, and NPC issuances	☐ Service providers are not honoring their compliance obligations (includes registering with the NPC)

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

NOTE on Registration (from Circular 17-01):

PIC or PIP shall provide the following registration information to the NPC by Sept. 9, 2017:

name and contact details of the PIC or PIP, head of agency or organization, and DPO.

PIC or PIP shall provide the following registration information to the NPC by March 8, 2018:

A. purpose or mandate of the government agency or private entity;

B. identification of all existing policies relating to data governance, data privacy, and information security, and other documents that provide a general description of privacy and security measures for data protection;

C. attestation regarding certifications attained by the PIC or PIP, including its relevant personnel, that are related to personal data processing;

D. brief description of data processing system or systems:

   a. name of the system;
   b. purpose or purposes of the processing;
   c. whether processing is being done as a PIC, PIP, or both;
   d. whether the system is outsourced or subcontracted, and if so, the name and contact details of the PIP;
   e. description of the category or categories of data subjects, and their personal data or categories thereof;
   f. recipients or categories of recipients to whom the personal data might be disclosed; and
   g. whether personal data is transferred outside of the Philippines;

E. notification regarding any automated decision-making operation.

Why the focus on automated decision-making?

- Historical Trends
  - If-Then/Case Processing
  - Expert Systems/Neural Networks
  - Machine Learning/Deep Learning
- Human Nature (to delegate)
  - Payroll Processing to Performance Ratings
  - Loan Applications to College Admissions
  - Jail Terms to Determination of Guilt
  - Route Navigation to Self-driving
- Why NPC (why not DICT)
  - RA 10173 gives Data Subjects the "Right to Object"
- NPC will investigate on how Personal Data was used for Automatic Processing
  - Source/s of data used (consent)
  - Storage of data (usually in the cloud)
  - Over-collection (collectivitis)
  - Biased data sets (patternitis)
  - Auditability and transparency (black box)
  - Re-identification (forest for the trees)

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Summary:
What compliance looks like

1. **Registration of DPO with the NPC**
   by September 9, 2017
2. **Registration of automated processes, etc.**
   by March 8, 2018
3. **Privacy impact assessments**
   ASAP, conducted by the process owners
4. **Breach team and procedures in place**
   ASAP, after conduct of PIA
5. **Privacy policies and data protection measures**
   ASAP, disseminated within the organization
6. **PIP contracts / data sharing agreements**
   ASAP, with assistance from Legal
7. **Notification to NPC within 72 hours**
   ASAP, in the event of a personal data breach

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

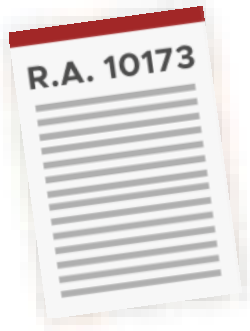
How should you comply?

- Sectors can craft their own **"privacy codes"** to address relevant industry issues and practices. These codes can be submitted to the NPC for review/comment.
- Sectoral Code for Education sector can address the following common concerns:
  - DPO Training and Certifications
  - Data sharing with CHED, PRC, etc.
  - Standards for Research Ethics Boards
  - Publishing list of top students/passers
  - Parent/student disputes

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

Crafting a sectoral code



- SEC. 7.j The NPC can Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers:
- *Provided,* That the privacy codes shall adhere to the underlying data privacy principles embodied in this Act:
- *Provided, further,* That such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller.
- For this purpose, the Commission shall consult with relevant regulatory agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law:
- *Provided, finally.* That the Commission may review such privacy codes and require changes thereto for purposes of complying with this Act.

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

What happens if you don't comply?

Sec. 7. Functions of the National Privacy Commission

(b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report...

(c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;

(d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;

(i) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act;

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION

What happens if you don't comply?

chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341

THE CHRONICLE OF HIGHER EDUCATION NEWS OPINION DATA ADVICE JOBS

SECTIONS FEATURED: The Far Right Comes to Campus Get the Teaching Newsletter Your Daily Briefing The Trends Report

TECHNOLOGY

High-profile data breaches cost institutions more than dollars and cents, according to college officials and data-security experts. There are also what some describe as "opportunity losses" and "reputational costs." These can include the embarrassment of having to explain an incident to parents, alumni, trustees, and prospective students.

"Higher ed is an active target," Ms. Bates says.

"It is not like people are accidentally happening upon us. They are actively pursuing us and trying to get our data."

Indiana U.

At Indiana U.'s data center, in Bloomington, staff members were aghast to learn that the university was among several in recent weeks to come upon security breaches in their information-technology operations.

Remember:

You are a TARGET!

DP FOR THE ACADEME 4

NATIONAL PRIVACY COMMISSION