

DATA PRIVACY ACT OVERVIEW

Khane Samala-Raza
Public Information & Assistance Division

What is the right to privacy?

the right to be let alone—the most comprehensive of rights and the right most valued by civilized men

[Brandeis J, dissenting in *Olmstead v. United States*, 277 U.S. 438 (1928)]

WHY IS IT IMPORTANT?



1004



30



2



0



1



Public school teacher in debt because of identity theft

Published February 26, 2016 10:48pm

A public school teacher may be a victim of identity theft as he owes three banks P800,000 for loans he did not apply for, according to a report by John Consulta on GMA-7's "24 Oras" on Friday.

Mark Joseph Lontok said he received notifications from three banks saying that he borrowed a total of P800,000 in salary loans. He denied applying for the loans.

Mark Joseph Lontok said he received notifications from three banks saying that he borrowed a total of P800,000 in salary loans. He denied applying for the loans.

However, Lontok remembered posting a photo of his Professional Regulation Commission (PRC) ID online.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION



DATA PRIVACY ACT *of* 2012

DPA sections



SECTION 1 - 6

Definitions
and General
Provisions



SECTION 7 - 10

National
Privacy
Commission



SECTION 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

KEY TERMS

KEY TERMS



PERSONAL INFORMATION

KEY TERMS



SENSITIVE PERSONAL INFORMATION

KEY TERMS



PRIVILEGED INFORMATION

PRIVILEGED INFORMATION

Data received within the context of a protected relationship

Husband and Wife

Priest and Penitent

Attorney and Client

Doctor and Patient

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

KEY TERMS



PERSONAL DATA

KEY TERMS



DATA SUBJECT

KEY TERMS



PERSONAL INFORMATION CONTROLLER

KEY TERMS



PERSONAL INFORMATION PROCESSOR

KEY TERMS



DATA PROCESSING SYSTEM

KEY TERMS



DATA SHARING

YOUR OBLIGATIONS

under the DATA PRIVACY ACT

OBLIGATION 1: **Adhere to data privacy principles**

TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY



Notice to the Participants

For this DPO Assembly, we collected your names, email addresses and company affiliation when you registered for purposes of coordination and printing of certificates. Through this attendance sheet, we also collect your signature as proof of attendance. We also request your consent to take and use your photos for online and offline communication materials; to use your contact address you provided for purposes of sending you online NPC communication materials. You have the option not to give us your consent by checking the 'No' option in the columns below. You may revoke your authorizations at any time by notifying us via info@privacy.gov.ph. All personal information collected will be stored in a secure location and only authorized staff will have access to them.

I agree

I do not agree

OBLIGATION 2: **Uphold**
data subject rights

INFORMATION



OBJECT



ACCESS



CORRECT



ERASE



DAMAGES



DATA PORTABILITY



FILE A COMPLAINT

OBLIGATION 3: **Implement
security measures**

ORGANIZATIONAL

TECHNICAL

PHYSICAL



NPC ISSUANCES

CIRCULARS

NPC Circular 16-01 – Security of Personal Data in Government Agencies

NPC Circular 16-02 – Data Sharing Agreements Involving Government Agencies


NPC Circular 16-03 – Personal Data Breach Management

NPC Circular 16-04 – Rules of Procedure


NPC Circular 17-01 – Registration of Data Processing Systems

NPC Circular 17-01 Appendix 1 – Registration of Data Processing Systems Appendix 1

ADVISORIES

 NPC Advisory No. 2017-01 – Designation of Data Protection Officers

 NPC Advisory No. 2017-02 – Access to Personal Data Sheets of Government Personnel

 NPC Advisory No. 2017-03 – Guidelines on Privacy Impact Assessments

PENALTIES

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

PENALTIES

PUNISHABLE ACT	JAIL TERM	FINE (PESOS)
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

5 PILLARS OF DATA PRIVACY ACCOUNTABILITY & COMPLIANCE



1 Appoint a Data Protection Officer



2 Conduct a Privacy Impact Assessment



3 Create a Privacy Management Program



4 Implement Data Privacy and Security Measures



5 Be ready in case of a Data Breach



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in

QUIZ



NATIONAL PRIVACY COMMISSION

THE

D P O

DATA PROTECTION OFFICER

WHAT IS A DPO?



Individual(s) accountable for ensuring PICs / PIPs' compliance with the DPA, its IRR, NPC Issuances & other applicable laws

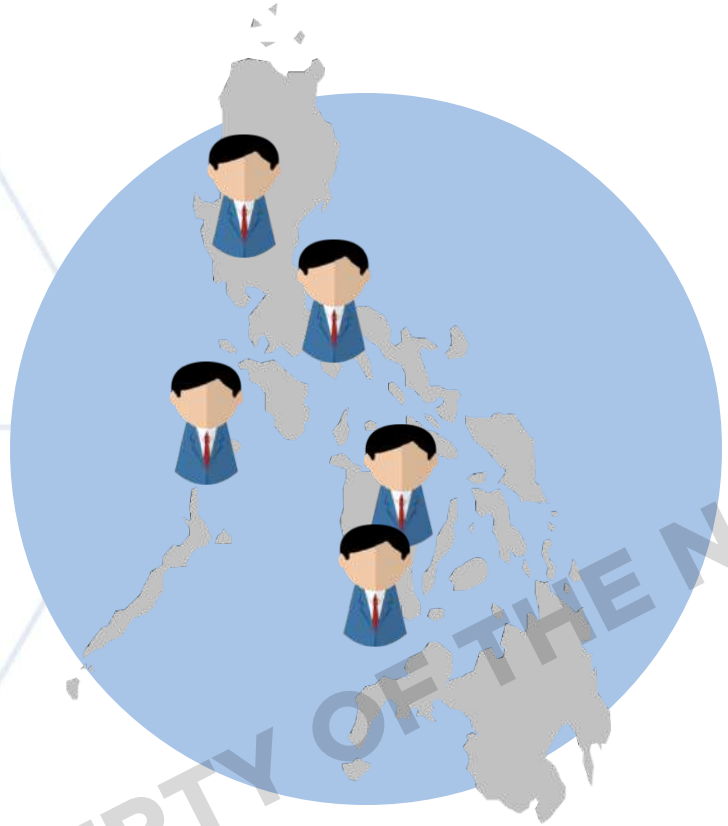
WHAT IS A COMPLIANCE OFFICER FOR PRIVACY?



Individual(s) who perform some of the functions of a DPO in particular cases:

- LGUs
- Gov't agencies
- Private sector (subject to NPC approval)
- Analogous cases

WHY APPOINT A DPO?



- ✓ A legal requirement
- ✓ A cost-efficient solution to achieve compliance & accountability
- ✓ Extra beneficial for PICs/PIPs with cross-border personal data transfers

WHY BE A DPO?

s-cyber-gdpr-dpo/rise-of-the-data-protection-officer-the-hottest-tech-ticket-in-town-idUSKCN1FY1MY

CYBER RISK FEBRUARY 14, 2018 / 8:11 PM / 13 DAYS AGO

Rise of the data protection officer, the hottest tech ticket in town

Salvador Rodriguez 5 MIN READ  

SAN FRANCISCO (Reuters) - They may not have the cachet of entrepreneurs, or geek chic of developers, but data protection officers are suddenly the hottest properties in technology.



GENERAL PRINCIPLES



- Responsibility lies with the PIC or PIP, not with the DPO
- Autonomy of the DPO or COP in the performance of duties
- Confidential nature of the position

ROLES AND FUNCTIONS



1. Monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the NPC & other applicable laws and policies.

ROLES AND FUNCTIONS



2. Ensure the conduct of **Privacy Impact Assessments** relative to activities, measures, projects, programs, or systems of the PIC or PIP;

ROLES AND FUNCTIONS



3. Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights

ROLES AND FUNCTIONS



4. Ensure **proper data breach and security incident management** by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;

ROLES AND FUNCTIONS



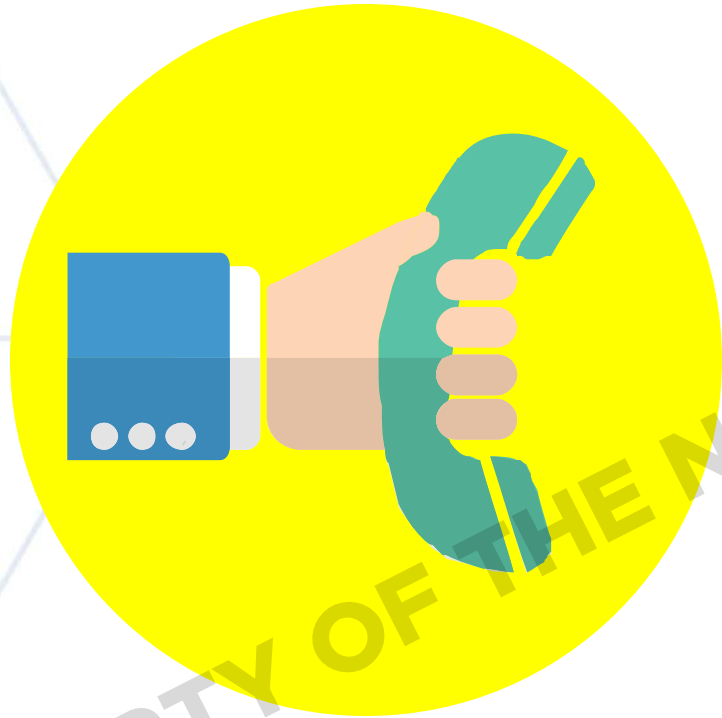
5. Inform & cultivate **awareness** on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;

ROLES AND FUNCTIONS



6. Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;

ROLES AND FUNCTIONS



7. Serve as the **contact person** of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;

ROLES AND FUNCTIONS



8. Cooperate, coordinate & seek advice of the NPC regarding matters concerning data privacy and security; and

ROLES AND FUNCTIONS

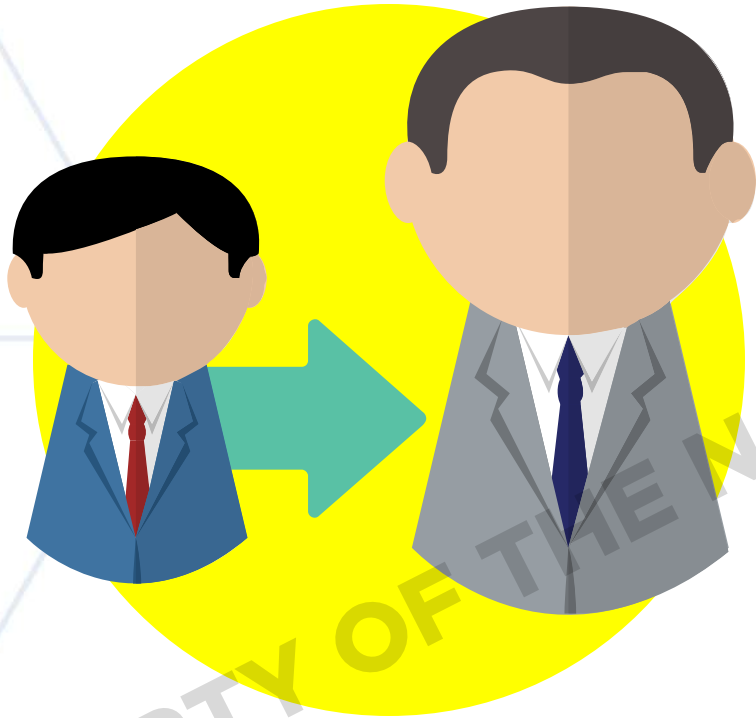


9. Perform other duties & tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security & uphold the rights of the data subjects

ROLES AND FUNCTIONS (FOR COPs)

- Except for items (1) to (3), a COP shall perform all other functions of a DPO
- assist the supervising DPO in the performance of the latter's functions.

SUBCONTRACTING THE FUNCTIONS OF DPO/COP



- Outsourcing or subcontracting of DPO functions is allowed.
- DPO or COP must oversee the performance of the third-party service provider.
- DPO or COP shall remain the contact person

SKILLS*



- **Interpersonal & communication skills**
- **Advanced org'l & privacy program mgt skills**
- **Advanced leadership skills**

SKILLS*



- **Data privacy strategy skills**
- **Business skills**
- **External engagement skills**

SUPPORTING THE DPO



- **Top management**
- **Process owners**
- **Human resource**
- **Legal division**
- **IT**
- **Security**
- **Internal Audit**



Republic of the Philippines
National Privacy Commission
REGISTRATION OF DATA PROCESSING SYSTEM
DATA PROTECTION OFFICER – DPO



Note: The personal information submitted herein shall be used for the initial phase of the Data Processing System Online Registration and supporting documents should be attached along with this form. Once this form has been validated by the NPC, you will be given an access code via email and SMS to continue with your registration with the online system. You may find the list of supporting documents in our guidelines forwarded to you via email and posted in our website.

All the information submitted herein shall be used for the purpose stated above and other legitimate interest of NPC as mandated by law. Information that are matters of public interest may be disclosed to the public. Rest assured that security controls are implemented to protect all the information in this document.

PERSONAL INFORMATION CONTROLLER / PERSONAL INFORMATION PROCESSOR

NAME OF ORGANIZATION _____

WEBSITE (URL) _____ EMAIL ADDRESS _____

COMPANY ADDRESS _____ CONTACT NO. _____

HEAD OF THE ORGANIZATION

LAST NAME _____ EMAIL ADDRESS _____

FIRST NAME _____ CONTACT NO. _____

MIDDLE INITIAL _____

OFFICIAL DESIGNATION _____

DATA PROTECTION OFFICER

LAST NAME _____ EMAIL ADDRESS _____

FIRST NAME _____ TEL. NO. _____

MIDDLE INITIAL _____ MOBILE NO. _____

OFFICIAL DESIGNATION _____ DATE OF DESIGNATION AS DPO _____

SWORN STATEMENT

I declare under oath that this Registration Form is accomplished by Data Protection Officer, and is a true, correct and complete statement and pursuant to the provision of the pertinent laws, rules and regulations of the Republic of the Philippines. I also authorize the National Privacy Commission to verify/validate the contents stated herein.

Head of Agency (Signature over Printed Name)

Data Protection Officer (Signature over Printed Name)

SUBSCRIBED and SWORN to before me, this _____, who exhibited to me (his/her) Government Issued ID No. _____ issued at _____ on _____

Notary Public

Doc. No. _____

Page No. _____

Book No. _____

Series of _____

*** TO BE FILLED UP BY NPC-COMPLIANCE AND MONITORING DIVISION ***

NPC ACCESS CODE	APPROVED BY (SIGNATURE OVER PRINTED NAME)
DATE GIVEN (MMDD/YYYY)	

REGISTRATION

with the **NPC**

WHO MUST REGISTER?

Any professional or organization must register if:

- A** It has 250 or more employees
- B** It processes sensitive personal information of 1,000 or more individuals
- C** Its processing may likely pose a risk to the rights and freedoms of data subjects
- D** Its processing is 'not occasional'

WHO MUST REGISTER?

Any professional or organization must register if they belong to one of the following sectors:

- 1** Government branches, bodies or entities, including NGAs, bureaus or offices, constitutional commissions, LGUs, GOCCs
- 2** Banks and non-bank financial institutions, including pawnshops, non-stock savings and loan associations (NSSLAS)
- 3** Telco networks, internet service providers and other entities or organizations providing similar services
- 4** Business process outsourcing
- 5** Universities, colleges and other institutions of higher learning, all other schools and training institutions

WHO MUST REGISTER?

Any professional or organization must register if they belong to one of the following sectors:

- 6 Hospitals including primary care facilities, multi-specialty clinics, custodial care facilities, diagnostic or therapeutic facilities, specialized out patient facilities, and other organizations processing genetic data
- 7 Providers of insurance undertakings, including life and nonlife companies, pre-need companies and insurance brokers
- 8 Business involved mainly in direct marketing, networking, and companies providing reward cards and loyalty programs
- 9 Pharmaceutical companies engaged in research
- 10 Personal information processors processing personal data for a personal information controller included in the preceding items, and data processing systems involving automated decision-making

WHY SHOULD YOU REGISTER?

- **A legal requirement**
- **Good for your brand**
- **Boosts compliance readiness in several ways**

HOW TO REGISTER?



PAPER DOCUMENTS - GOV'T

2 Original hard copies



- Certified true copy of the Special/Office Order, or any similar document, designating or appointing the DPO of the PIC or PIP; and
- Where applicable, a copy of the charter of your agency, or any similar document identifying its mandate, powers, and/or functions

PAPER DOCUMENTS - PRIVATE

2 Original hard copies

- Duly-notarized Secretary's Certificate authorizing the appointment or designation of DPO, or any other document that demonstrates the validity of the appointment or designation
- Certified true copy of any of the following documents, where applicable:
 - Certificate of Registration (SEC Certificate, DTI Certification of Business Name or Sole Proprietorship) or any similar document; and/or
 - Franchise, license to operate, or any similar document.

Phase 2 Checklist

To complete your **Phase 2 Registration**, prepare the following info per data processing system (DPS), in advance:

- Your DPS name
- Info on whether you manage the DPS as a PIC, PIP or both
- Type of DPS (manual/paper-based, electronic or both).
If electronic or both, info on whether:
 - a. the process involves fully automated decision making
 - b. the decision will significantly affect the data subject

- Purpose(s)/Description of the DPS
- Info on whether the personal data processed in the DPS will be transferred outside the Philippines
- Info on whether the DPS is subcontracted/outsourced or not. If yes, info on the following:
 - a. Personal information processor (PIP) name
 - b. PIP email
 - c. PIP address
 - d. PIP contact number & local extension number
 - e. PIP description
- Categories of data subjects (employees, students, patients, clients, etc.)
- Info as to whom the personal data will be disclosed, including the organization type



WHEN SHOULD YOU REGISTER?

- PHASE II- 8 March 2018
- Annually renewable w/in 2 months prior to, but not later than 8 March
- Amendment or updates to be made w/in 2 months from the date such changes take into effect