NATIONAL PRIVACY COMMISSION

Primer on the Data Privacy Act (DPA) of 2012

ABCD-S: "**A**wareness, **B**reach Management, **C**ompliance, **D**ata Protection Officer and **S**ecurity Measures“

NCR – School Registrars’ Association (NACSRA)

November 24, 2017

Dr. Rolando R. Lansigan
Chief, Compliance and Monitoring Division
National Privacy Commission (NPC)


ANIMO


© Hazel Thompson

Do not COLLECT if you cannot PROTECT

ВОТРА

Who stores data about you?

facebook

YouTube

Google

powered by ebay.co.uk

HSBC

The world's local bank

SM

SPEED OF
INFORMATION

Which is more valuable?

Data

Money

“Data is more valuable than Money. If someone takes your money, that's all they have. If you let someone take your data, they may eventually take your money too!“

from: Deputy Privacy Commissioner Dondi Mapa

NATIONAL PRIVACY COMMISSION

In today's environment,
where competitors can copy your products, pirate your employees, and mirror your algorithms,
data is the only
sustainable competitive advantage.

FORMER
DEPUTY PRIVACY
COMMISSIONER
DAMIAN MAPA

What is the Data Privacy Act of 2012?

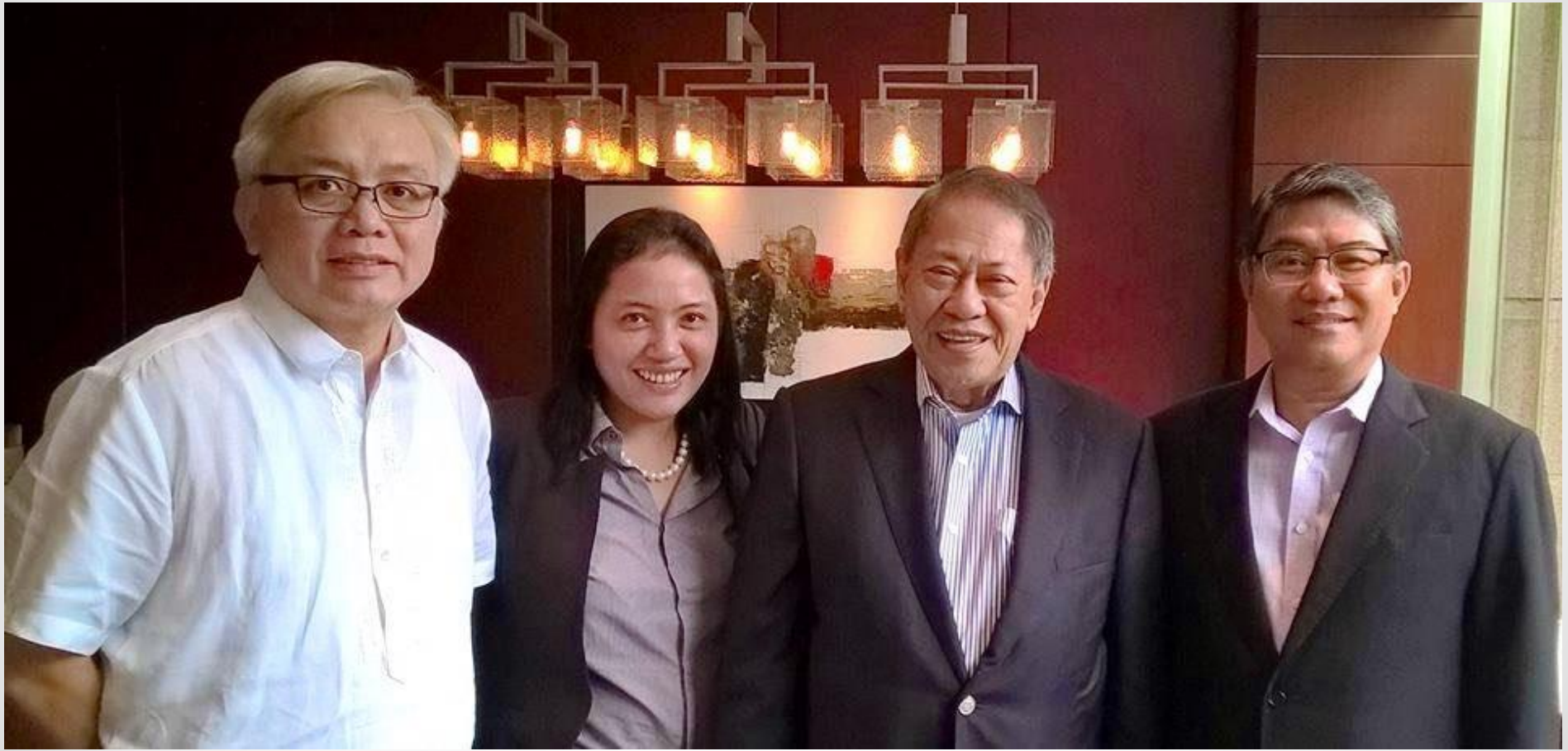
- SECTION 1. Short Title. – This Act shall be known as the “Data Privacy Act of 2012”.

- Republic Act 10173, the Data Privacy Act of 2012

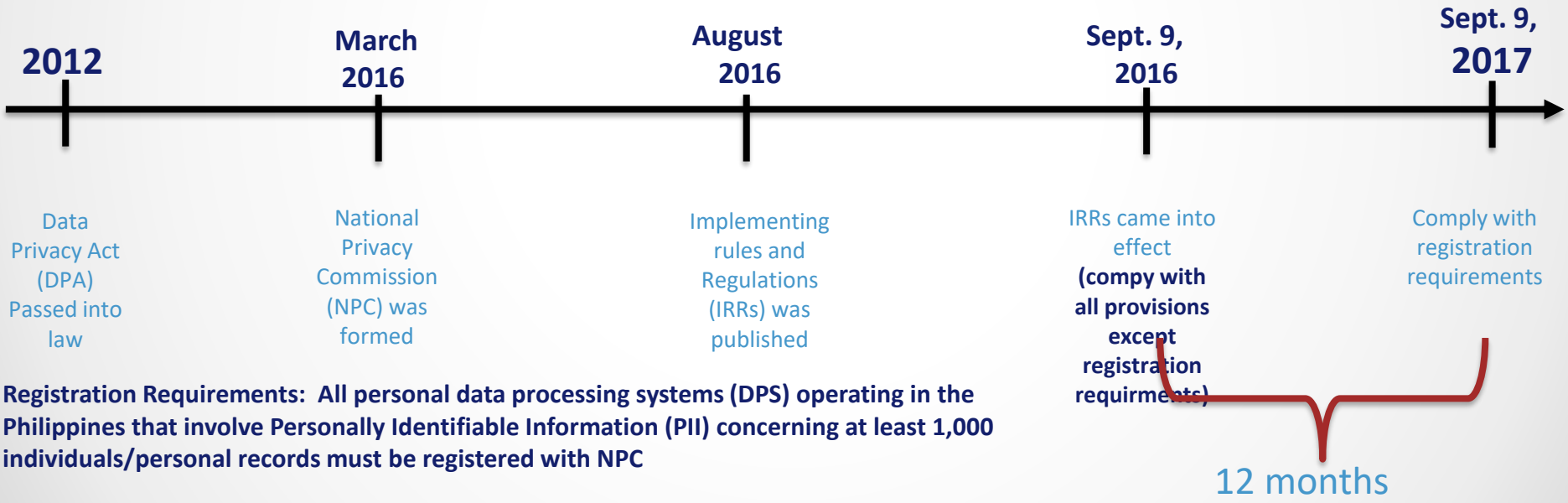
AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

- The National Privacy Commission (NPC) is a body that is mandated to administer and implement this law. The functions of the NPC include:
  - rule-making,
  - advisory,
  - public education,
  - compliance and monitoring,
  - investigations and complaints,
  - and enforcement.

Main Author of R.A. 10173 and the NPC Commissioners



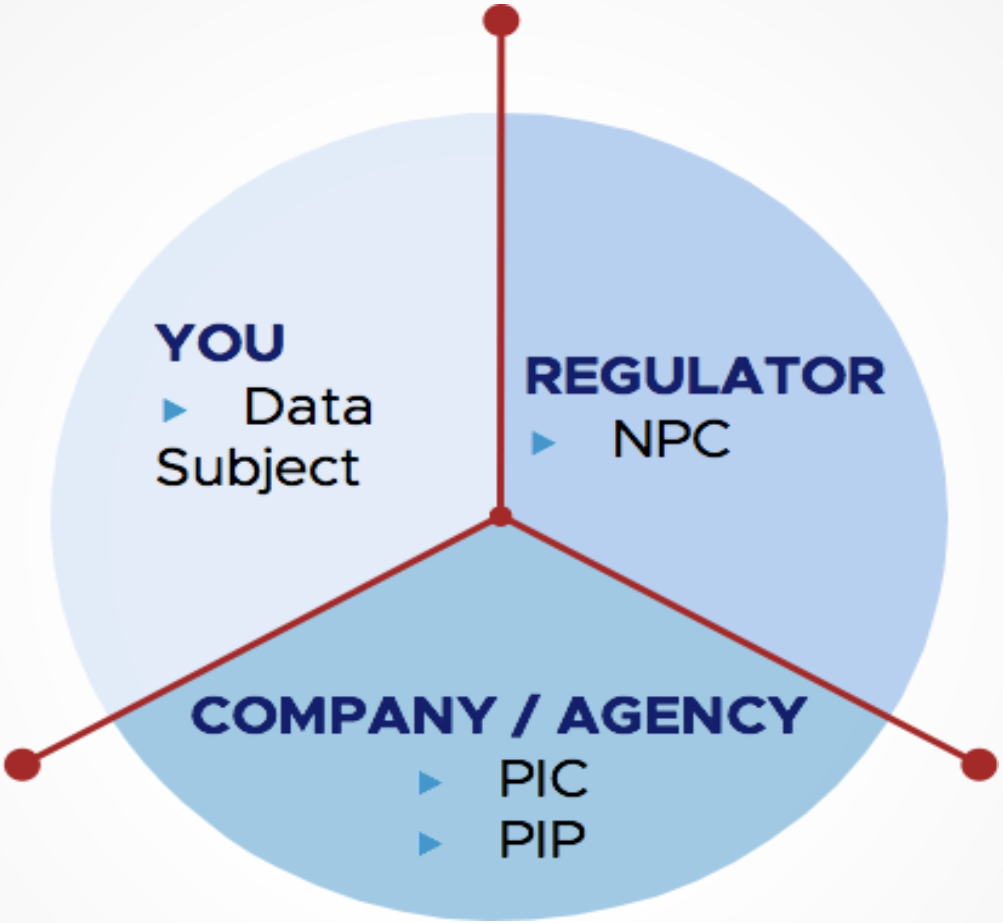
Timeline of DPA Law and IRRs passed to Organization's Compliance



Registration Requirements: All personal data processing systems (DPS) operating in the Philippines that involve Personally Identifiable Information (PII) concerning at least 1,000 individuals/personal records must be registered with NPC

KEY ROLES IN THE DATA PRIVACY ACT

- **Data Subjects**
  - Refers to an individual whose, sensitive personal, or privileged information is processed personal
- **Personal Information Controller (PIC)**
  - Controls the processing of personal data, or instructs another to process personal data on its behalf.
- **Personal Information Processor (PIP)**
  - Organization or individual whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject
- **Data Protection Officer (DPO)**
  - Responsible for the overall management of compliance to DPA
- **National Privacy Commission**
  - Independent body mandated to administer and implement the DPA of 2012, and to monitor and ensure compliance of the country with international standards set for personal data protection


YOU
Data Subject
REGULATOR
NPC
COMPANY / AGENCY
PIC
PIP

Examples of Breaches and Live Cases

1. COMELeak (1 and 2)
2. BPI – consent form
3. Hospital – unsecure storage records
4. Student transferred by her parent without her knowledge
5. Clinical record of a student to disclose with her parents
6. List of top students/passers
7. Known Fastfood delivery – disclosing personal info of clients
8. No Data sharing agreement (DSA) between and among Schools and Universities
9. Cedula in malls
10. Security issues in buildings – logbook
11. Profiling of customers from a mall
12. Unjustifiable collection of personal data of a school
13. No Privacy Notice
14. Use of USB
15. Privacy notice
16. Use of USB
17. Personal laptop stolen
18. Lost a CD in transit
19. An error in viewing of student records in the online system
20. Use of re-cycled papers
21. Raffle stubs
22. Universities and Colleges websites with weak authentication
23. Personal Records stolen from home of an employee
24. Photocopiers re-sold without wiping the hard drives
25. Release of CCTV Footage
26. Hard drives sold online
27. Password hacked/revealed
28. Unencrypted Data

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

NATIONAL PRIVACY COMMISSION

Potential Penalties listed in the Data Privacy Act

DPA Section	Punishable Act	For Personal Information	For Sensitive Personal Information	Fine (Pesos)
		JAIL TERM		
25	Unauthorized processing	1-3 years	3-6 years	500 k – 4 million
26	Access due to negligence	1-3 years	3-6 years	500 k – 4 million
27	Improper disposal	6 months – 2 years	3-6 years	100 k – 1 million
28	Unauthorized purposes	18 months – 5 years	2-7 years	500 k – 2 million
29	Intentional breach	1-3 years		500 k – 2 million
30	Concealment of breach	18 months – 5 years		500 k – 1 million
31	Malicious disclosure	18 month – 5 years		500 k – 1 million
32	Unauthorized disclosure	1-3 years	3-5 years	500 k – 2 million
33	Combination of acts	1-3 years		1 million – 5 million

Top 20 Government-imposed Data Privacy Fines Worldwide, 1999-2014 **

Rank	Fined entity	Amount of fines and penalties	Year	Country	Privacy principles violated
1	Apple	$32.5M	2014	U.S.	Choice and Consent
2	Google	$22.5M	2012	U.S.	Collection
3	Google	$17M	2013	U.S.	Collection and Notice
4	ChoicePoint	$15M	2006	U.S.	Security
5	Hewlitt-Packard	$14,5M	2006	U.S.	Collection
6	LifeLock	$12M	2010	U.S.	Accuracy, Security
7	TJ Maxx	$9.8M	2009	U.S.	Security
8	Dish Network	$6M	2009	U.S.	Choice and Consent
9	DirecTV	$5.3M	2005	U.S.	Choice and Consent
10	HSBC	$5M	2009	UK	Security
11	US Bancorp	$5M	1999-2000	U.S.	Disclosure
12	Craftmatic	$4.3	2007	U.S.	Choice and Consent
13	Cignet Health	$4.3M	2011	U.S.	Access
14	Barclays Bank	$3.8M	2013	U.S.	Use and Retention
15	Certegy Check Services	$3.5M	2013	U.S.	Accuracy
16	Playdom	$3M	2011	U.S.	Collection and Notice
17	The Broadcast Team	$2.8M	2007	U.S.	Collection
18	Equifax, TransUnion and Experian	$2.5M	2000	U.S.	Access
19	CVS Caremark	$2.3M	2009	U.S.	Security and Disposal
20	Norwich Union Life	$1.8M	2007	UK	Disclosure

**SOURCE IAPP 17 FEB 2014

Rights of the Data Subject

- Right to be informed - IRR, Section 34.a
- Right to object - IRR, Section 34.b
- Right to access - IRR, Section 34.c
- Right to data portability - IRR, Section 36
- Right to correct (rectification) - IRR, Section 34.d
- Right to erasure or blocking - IRR, Section 34.e
- Right to file a complaint - IRR, Section 34.a.2
- Right to damages - IRR, Section 34.f
- Transmissibility of Rights - IRR, Section 35

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:

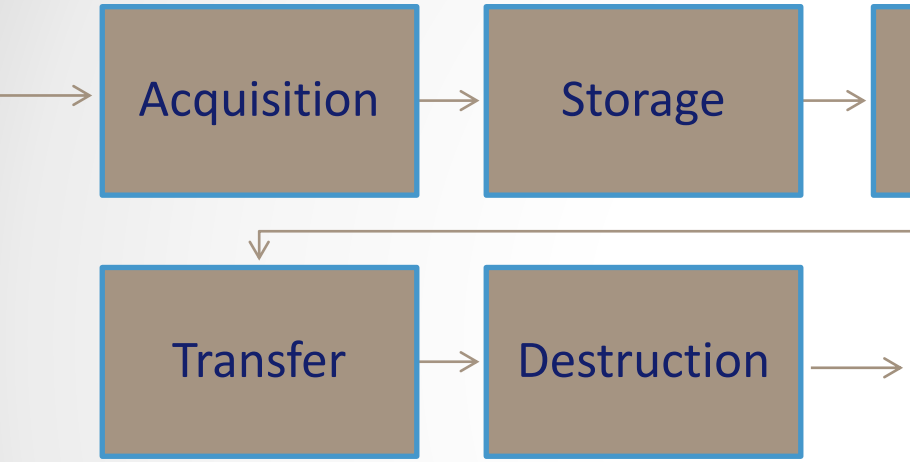
social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns;

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	
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

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

Personal Data Lifecycle

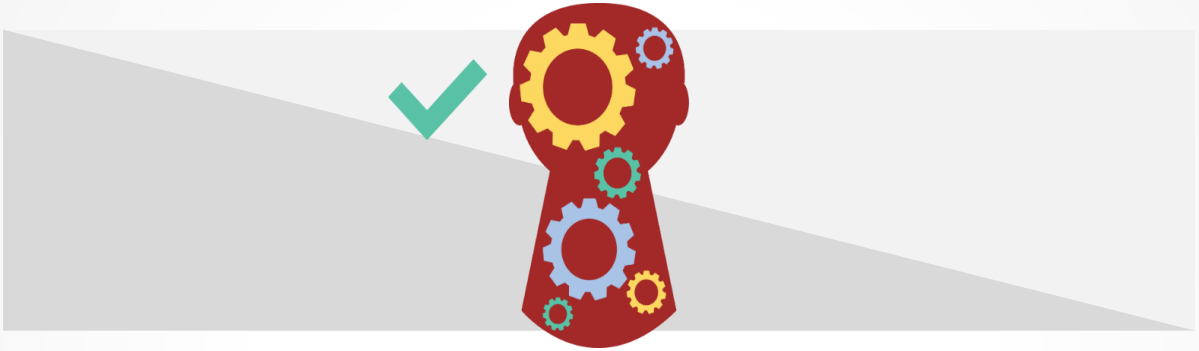


- Key considerations when listing your personal data:
  - What personal data do you collect?
  - In what form and through which channels?
  - For what purpose you collect personal data
  - How is it used?
  - Who is this data shared with internally and externally?
  - Who is authorized to access this data?
  - Where do you keep your data?
  - How long do you keep your data?
  - How do you dispose this data?

Retention/Disposal should be based on:

1. **Law**
2. **Industry Best Practice**
3. **Business Needs**

TRANSPARENCY – “the CONSENT Regime”



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.

Admissio Services

EXCHANGE STUDENTS

FOR THE S.Y. 2016-2017

THAILAND

KING MONGKUT'S UNIVERSITY OF TECHNOLOGY IN THONBURI *(KMUTT)*

MAE FAH LUANG UNIVERSITY *(MFU)*

APPLE MIE TAMAYO
BS CHEMICAL ENGINEERING
KMUTT

HYACINTH MAE CORTEZ
BS CHEMICAL ENGINEERING
KMUTT

KRISZELLE SHANE APOR
BS CHEMICAL ENGINEERING
KMUTT

ANA TRIXIA ORPINA
BS ACCOUNTANCY
MFU

MALAYSIA

UNIVERSITY OF MALAYA

UNIVERSITI TEKNOLOGI MALAYSIA *(UTM)*

ANDREA ROZE BASARTE
BS ACCOUNTANCY

MARLON JABLA II
BS ACCOUNTANCY

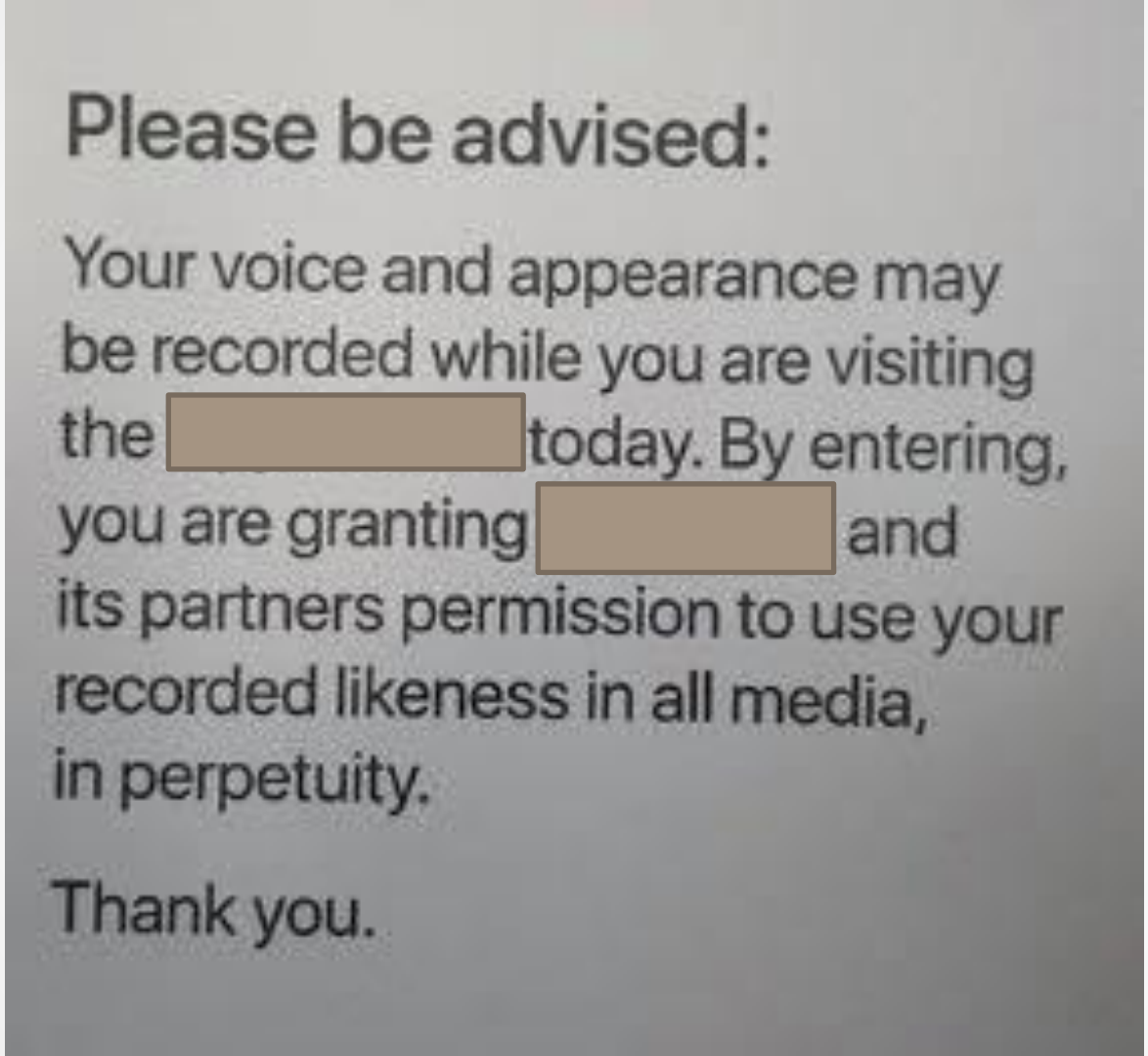
KENNETH JAY NORBERTE
BS ACCOUNTANCY

JAYKARL SAMAR
BS ELECTRICAL ENGINEERING

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.


Please be advised:
Your voice and appearance may be recorded while you are visiting the [redacted] today. By entering, you are granting [redacted] and its partners permission to use your recorded likeness in all media, in perpetuity.
Thank you.

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.

Avoid this mentality:
“just in case we need it”
“this is what we always do”

RECORDS AND ADMISSION CENTER

[ ] Main [ ] Branch _____

STUDENT GENERAL INFORMATION SHEET

(For Freshmen and Transferee)

A. PERSONAL PROFILE

Surname:			**Program intended to enroll:** Degree_____ Major _____
First Name:			
Middle Name:			
Birth Date:	Age:	Sex:	**Preferred class session:** [ ] Morning [ ] Afternoon [ ] Evening
Birth Place:	Civil Status:		
Religion:	Nationality:		**Documents submitted for admission:** • Form 138 [ ] • Birth Certificate (*NSO Certified*) [ ] • Good Moral Character [ ] • Honorable Dismissal [ ] • Transcript of Records (*info copy*) [ ] • Medical Certificate (*for Nursing, Midwifery & Caregiver*) [ ] • Others [ ]
Provincial Address:			
City Address:			
Contact No.*(Landline/Mobile)*:	Email Add:		

Do you have physical disabilities?
[ ] No [ ] Yes (if yes, please specify: _____)

B. FAMILY BACKGROUND

Name of Father:		Age:	Nationality:
Occupation/Position:	Employer's Name/Address:	Highest Educational Attainment:	
Name of Mother:		Age:	Nationality:
Occupation/Position:	Employer's Name/Address:	Highest Educational Attainment:	
Name of guardian *(if not staying with parents)*:		Age:	Nationality:
Contact No. *(Mobile)*: *(Landline)*:	Email Add:	No. of Siblings/Children:	

C. ACADEMIC PROFILE

Elementary	School Name:	
	Address:	
	Type: [ ] Private [ ] Public	Honor/s Received:
Secondary	School Name:	
	Address:	
	Type: [ ] Private [ ] Public	Honor/s Received:
Last Tertiary School Attended	School Name:	
	Address:	
	Type: [ ] Private [ ] Public	Honor/s Received:

D. SOCIO ECONOMIC AND CULTURAL PROFILE

D.1 You are a:

[ ] Professional/full-time student

[ ] Working Student

Nature of work: _____

D.2 You are living with:

[ ] Entire family

[ ] Both parents

[ ] Father alone

[ ] Mother alone

[ ] with Sister and/or Brother

[ ] with Relatives

[ ] – Aunt/Uncle

[ ] – with Grandparents

[ ] – with Cousin/s

[ ] Others _____

D.3 You are living in:

[ ] A boarding house [ ] An apartment

[ ] A room for rent [ ] A rented house

[ ] A house your family own

[ ] Others _____

D.4 Your studies is supported by:

[ ] Your parents

[ ] Your sister/brother

[ ] A relative

[ ] Scholarship

[ ] Others _____

D.5 Tribal Affiliation:

[ ] Tiboli [ ] Aeta

[ ] Manobo [ ] Mansaka

[ ] Bagobo [ ] Matigsalog

[ ] Bilaan [ ] Others:

[ ] Mandaya _____

D.6 The program you intended to enroll is

[ ] Your choice [ ] Friend's choice

[ ] Parent's choice [ ] Peer's choice [ ] Others

[ ] Relative's choice [ ] Sister's/Brother's choice _____

E. OTHER RELEVANT INFORMATION

E.1 Reasons for enrolling in UM (*Select three (3) and rank 1,2,3*):

[ ] [redacted] accredited programs
[ ] Easy installment plan
[ ] Term system
[ ] Highly qualified faculty
[ ] Affordable tuition fee
[ ] State-of-the-Art facilities
[ ] Others: _____

F. PERSON TO BE CONTACTED IN CASE OF EMERGENCY

Name: _____ Relation: _____

Address: _____ Contact No.: _____

_____ _____

Student's Signature Over Printed Name Date

The Approval for the enrolment of any student is automatically cancelled if the basis of acceptance he/she submitted is later found to be fraudulent. Any units earned since the time of acceptance is deemed null and void.

Applicant ID : 1718AT24249 **Applicant Name : AA, AA**

Personal Information

Instructions :
1. Kindly type 'NA' in boxes where there are no possible answers to the information being requested.
2. To make use of the letter 'Ñ', please press ALT while typing "165"; while for 'ñ', please press ALT while typing "164".

NO PHOTO UPLOADED

Classified As:

- ○ Freshman
- ○ Transferee
- ○ ETEEAP
- ○ Exchange Student
- ○ Cross Enrollee
- ○ Degree Holder
- ○ Second Courser

SAVE

Printer-friendly format (Note : Print application form in long bond paper)

PERSONAL DATA

Name	AA	AA	AA	
	* Last Name	* First Name	* Middle Name	* Extension Name

Program: - select course - View Academic Path

Date of Birth: 07/13/2017 Place of Birth: Age: 0

Gender: ○ Male ○ Female

Gender Preference (check if applicable) Non Binary (LGBT)

Nationality Status: - nationality status - Civil Status: - civil status -

Nationality: Filipino Nationality *for dual citizenship: - nationality -

Country: - Country -

Permanent Address: * (Permanent) Region: - region - (Permanent) Province: - province - (Permanent) Municipality: - municipality -

Zip Code: ZIP CODE

Permanent Address * (Permanent) Region - region - (Permanent) Province - province - (Permanent) Municipality - municipality -

Zip Code ZIP CODE

(Rm# Bldg./House#, Street, Brgy.)

Residential Tel No.: Cellphone Number:

Instructions : If there is no provincial address, select address same as residential address.

Provincial Address * (Provincial) Region - region - (Provincial) Province - province - (Provincial) Municipality - municipality -

(Rm# Bldg./House#, Street, Brgy.)

Provincial Tel No.:

Height(in feet and inches) Weight (in pounds)

Learner Reference Number (LRN)

QVR ESC

Mother Tongue - Select Option - Indigenous People - Select Option -

Email Address Religion - religion - Blood Type - blood type -

Facebook Account Twitter Account

Personal Website

Is Working Student

FAMILY DATA

Father's Name Occupation - select occupation -

Alumnus Employee N/A

Contact Number E-mail Address

Mother's Name Occupation - select occupation -

Alumnus Employee N/A

Contact Number E-mail Address

Birth Rank only child eldest middle youngest Living Condition - select status - Parent Status - select status -

Parent's Home Address Who's financing your education? - Select Status - If Others (please specify):

No. of Siblings Living Arrangement - select living arrange -

No. of Siblings

No. of Brothers

Brother(s)' With Income

If married, name of spouse

Occupation

Annual Family Income: please include salaries of father, mother and siblings - Annual Family Income -

Living Arrangement - select living arrange -

No. of Sisters

Sister(s)' With Income

No. of Children

SIBLINGS

Name	Age	Occupation / YearLevel

PERSON TO BE NOTIFIED IN CASE OF EMERGENCY

Guardian's Name

Guardian's Tel No.

Guardian's Address

Relationship:

Guardian's Cell #

EDUCATIONAL DATA

School Level	School Type	Name of School	Address	Grade / Program	Year Attended	Honors/Awards Received	General Average
-school level-	-school type-						

OTHER INFORMATION

Award/Talent

Organization Membership

Work Experience

Place of Work

Inclusive Date

FOR FOREIGN STUDENT ONLY

Passport No.

Date Issued

Place Issued

Type Of Visa

Visa Status

I-Card No:

Authorized Stay From to

Remarks

SAVE

Welcome, **DELA CRUZ, JUAN M ()** SIGN OUT

Applicant ID : 1718AT67253 **Applicant Name : DELA CRUZ, JUAN**

Instructions:

1. Kindly type 'NA' in boxes where there are no possible answers to the information being requested.
2. To make use of the letter 'Ñ', please press ALT while typing "165"; while for 'ñ', please press ALT while typing "164".

STEP 1 Personal Data | **STEP 2** Family Background | **STEP 3** Educational Attainment | **STEP 4** Other Info

PERSONAL INFORMATION

Name	:	DELA CRUZ	JUAN	M		
	:	Last Name	First Name	Middle Name		
Program	:	COLLEGE OF ARTS AND SCIENCES				
Course	:	BS INFO & COMM TECHNOLOGY (BS INFOTECH)				
Classified As	:	Freshman				
Date of Birth	:	2005-11-01	Gender	:	Male ○ Female ○	
Place of Birth	:	Place of birth	Civil Status	:	- civil status -	
Age	:	12	Citizenship	:	- nationality -	
Religion	:	- religion -				

Permanent/Provincial Mailing Address : Permanent/Provincial Mailing Address ZipCode : Zip Code

Contact Numbers : Present Mobile

Contact Numbers : Contact Numbers

Email Address : Email Address

Physical/Medical Disability : No Yes If Yes, specify Physical/Medical Disability

FOR FOREIGN STUDENT ONLY

Passport No. : Passport No Date Issued : Date Issued Place Issued : Place Issued

Type of Visa : Type of Visa Visa Status : Visa Status I-Card No : I-Card No

Authorized Stay : From To Remarks : Remarks

Next ->

Welcome, **DELA CRUZ, JUAN M ()** SIGN OUT

Applicant ID : 1718AT67253 **Applicant Name : DELA CRUZ, JUAN**

Instructions:

1. Kindly type 'NA' in boxes where there are no possible answers to the information being requested.
2. To make use of the letter 'Ñ', please press ALT while typing "165"; while for 'ñ', please press ALT while typing "164".

STEP 1 Personal Data **STEP 2** Family Background **STEP 3** Educational Attainment **STEP 4** Other Info

FAMILY BACKGROUND

		FATHER	MOTHER
Name	:	Father's Name	Mother's Name
Is parent still alive	:	YES NO	YES NO
Parent	:	Select Status	Select Status
Home Address	:	Father's Home Address	Mother's Home Address
Age	:	Father's Age	Mother's Age
Citizenship	:	- nationality -	- nationality -
Telephone Number	:	Father's Telephone Number	Mother's Telephone Number
Mobile	:	Father's Mobile Number	Mother's Mobile Number
Email Address	:	Father's Email Address	Mother's Email Address
Highest Educational Attainment	:	Select Education Attainment	Select Education Attainment

Occupation/Position	:	Father's Occupation	Mother's Occupation
Working as an OFW?	:	YES NO	YES NO
Business/Employer Name	:	Father's Business/Employer Name	Mother's Business/Employer Name
Gross Monthly Family Income	:	Select Family Income	Select Family Income
Number of Siblings	:	Brothers Sisters	
Spouse	:	Name: Spouse Name Age: Spouse Age Occupation: Spouse Occupation	
No. Of Children	:	No. Of Children	

RELATIVES INFORMATION

Do you have relatives who are attending or have attended [redacted] Givenames, relationship and if possible, date of attendance.

Names	Relationship	Dates of Attendance
Name	Relationship	Date

<- Back

Next ->

[redacted]

Welcome, **DELA CRUZ, JUAN M ()** SIGN OUT

Applicant ID : 1718AT67253 **Applicant Name : DELA CRUZ, JUAN**

Instructions:

1. Kindly type 'NA' in boxes where there are no possible answers to the information being requested.
2. To make use of the letter 'Ñ', please press ALT while typing "165"; while for 'ñ', please press ALT while typing "164".

STEP 1 Personal Data **STEP 2** Family Background **STEP 3** Educational Attainment **STEP 4** Other Info

EDUCATIONAL ATTAINMENT

Please accomplish from elementary level up to the highest level attained.

School Level	Name of School	Address	Course	Major	Academic Year	Honors / Awards Recieved	Grade Level
Primary (Grade 4)	Name of School	Address	Course	Major	Academic Year	-Honors/Awards-	Grade Level
Intermediate (Grade 6)	Name of School	Address	Course	Major	Academic Year	-Honors/Awards-	Grade Level
High School	Name of School	Address	Course	Major	Academic Year	-Honors/Awards-	Grade Level
College	Name of School	Address	Course	Major	Academic Year	-Honors/Awards-	Grade Level
Masteral	Name of School	Address	Course	Major	Academic Year	-Honors/Awards-	Grade Level
Doctoral	Name of School	Address	Course	Major	Academic Year	-Honors/Awards-	Grade Level
Vocational Technology	Name of School	Address	Course	Major	Academic Year	-Honors/Awards-	Grade Level

Scholarships Recieved:

Have you been placed under probation? : Yes No If Yes, Academic Discipline

Have you ever been dismissed? : Yes No If Yes, Explain

Membership in Professional, Civil Societies, Associations, Labor Unios, etc. :

FOR APPLICANTS OF COLLEGE OF MEDICINE AND COLLEGE OF LAW.

1. **For College of Medicine only:** Have you taken NMAT? Yes No If yes, indicate NMAT Score: Score Date Taken mm/dd/yy

Note: If no, take the NMAT. It is a requirement

2. What other medical/law schools have you applied into?

3. Have you previously enrolled to other medical/law school? Yes No

If yes, indicate school: School

4. Have you eve been dismissed or disqualified from enrolling in that medical/law school by reason of scholastic standing or disciplinary action? Yes No

If yes, Explain:

5. Licensing Exam/s Passed:

<- Back

Next ->

Welcome, **DELA CRUZ, JUAN M ()** SIGN OUT

Applicant ID : 1718AT67253 **Applicant Name : DELA CRUZ, JUAN**

Instructions:

1. Kindly type 'NA' in boxes where there are no possible answers to the information being requested.
2. To make use of the letter 'Ñ', please press ALT while typing "165"; while for 'ñ', please press ALT while typing "164".

STEP 1 Personal Data | **STEP 2** Family Background | **STEP 3** Educational Attainment | **STEP 4** Other Info

WORK EXPERIENCE (start from the present)

Company Name	Company Address	Position	Date Employed	Tel./Cel. No/Fax No
Company Name	Company Address	Position	Date Employed	Tel./Cel. No/Fax No

How did you come to know

- ☐ from parents/siblings
- ☐ from my friends/classmates
- ☐ from my own initiative
- ☐ from teachers
- ☐ from the internet/webpage
- ☐ from brochures/poster
- ☐ from career orientation talks
- ☐ Others (pls. specify)

I have read and understood the admission policies of the College of Arts and Science.
I hereby apply for admission to the College of Arts and Science with the understanding that my application will be evaluated based on the policies set by the department.
If admitted, I agree to abide by its regulations.

I certify that the foregoing information and the credentials submitted are true and complete to the best of my knowledge.

THE FIVE PILLARS OF COMPLIANCE

NATIONAL PRIVACY COMMISSION

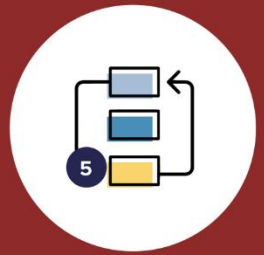
Commit to Comply: Appoint a **Data Protection Officer (DPO)**

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

Be Accountable: Create your **Privacy Management Program** and **Privacy Manual**

NATIONAL PRIVACY COMMISSION

Demonstrate Your Compliance: Implement your **privacy and data protection (PDP)** measures.



Be Prepared for Breach: Regularly exercise your **Breach Reporting Procedures (BRP)**.

Other Requirements

- Annual Breach Drill
- ❑ **Notification to NPC within 72 hours**
- ❑ **(in the event of a personal data breach)**
- Annual Breach Report
- Security Clearance
- Privacy Notice
- Data Sharing Agreement (DSA), if applicable
- Sub-contracting Agreement / Outsourcing Agreement

Data sharing checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis

Is the sharing justified?
Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?
Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Privacy notice

- **What information is being collected?**
- **Who is collecting it?**
- **How is it collected?**
- **Why is it being collected?**
- **How will it be used?**
- **Who will it be shared with?**

The Data Privacy Principles

- Personal data shall be:
  1. processed fairly and lawfully
  2. processed only for specified, lawful and compatible purposes
  3. adequate, relevant and not excessive
  4. accurate and up to date
  5. kept for no longer than necessary
  6. processed in accordance with the rights of data subjects
  7. kept secure
  8. shared to other PICs only if there is a DSA.

Self-help checklist on data protection policy

Remember: you should be able to answer YES to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

Rule 1: Fair obtaining:

- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them
- Can we describe our data-collection practices as open, transparent and up-front?

Rule 2: Purpose specification

- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?
- If we are required to register with NPC, does our register entry include a proper, comprehensive statement of our purpose? *[**Remember, if you are using personal data for a purpose not listed on your register entry, you may be committing an offence.**]*
- Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?

Self-help checklist on data protection policy

Remember: you should be able to answer YES to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

Rule 3: Use and disclosure of information

- Are there defined rules about the use and disclosure of information?
- Are all staff aware of these rules?
- Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.
- If we are required to register with NPC, does our register entry include a full list of persons to whom we may need to disclose personal data? *[Remember, if you disclose personal data to someone not listed on your register entry, you may be committing an offence.]*

Rule 4: Security

- Is there a list of security provisions in place for each data set?
- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data we keep?
- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files securely locked away from unauthorized people?

Self-help checklist on data protection policy

Remember: you should be able to answer YES to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

Rule 5: Adequate, relevant and not excessive

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard?

Rule 6: Accurate and up-to-date

- Do we check our data for accuracy?
- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?

Self-help checklist on data protection policy

Remember: you should be able to answer YES to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

Rule 7: Retention time

- Is there a clear statement on how long personal data are to be retained?
- Are we clear about any legal requirements on us to retain data for a certain period?
- Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?
- Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Rule 8: The Right of Access

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures guarantee compliance with the RA 10173 requirements?

Self-help checklist on data protection policy

Remember: you should be able to answer YES to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

Registration

- Are we clear about whether or not we need to be registered with the NPC?
- If registration is required, is the registration kept up to date? Does the registration accurately reflect our practices for handling personal data? *[Remember, if your data-handling practices are out of line with the details set out in your register entry, you may be committing an offence.]*

Training & Education

- Do we know about the levels of awareness of data protection in our organization?
- Are our staff aware of their data protection responsibilities - including the need for confidentiality?
- Is data protection included as part of the training program for our staff?

Self-help checklist on data protection policy

Remember: you should be able to answer YES to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

Co-ordination and Compliance

- Has a Data Protection Officer (DPO) / Compliance Officer for Privacy (COP) been appointed?
- Are all staff aware of his or her role?
- Are there mechanisms in place for formal review by DPO activities within our organization?
- Is the Privacy Impact Assessment (PIA) carefully planned and executed according to its purpose?
- Is there a Breach Management Program (BMP) in place?

Other Requirements

- Annual Breach Drill
  - **Notification to NPC within 72 hours (in the event of a personal data breach)**
- Annual Breach Report
- Security Clearance
- Privacy Notice
- Data Sharing Agreement (DSA), if applicable
- Sub-contracting Agreement / Outsourcing Agreement

1 Technical

2 Organisational – other measures

Technical

Encryption

To what standard? (cost Vs benefit)

All devices or just some?

Passwords

Enforced strength and updates?

Sharing data

Technical solutions – e.g. via email; portals

System testing & maintenance

Who has access, to what (System Administrators)

Live or dummy data?

Firewalls / Anti-virus / Spam filters

Backups

Secure: encrypted tapes | cloud-provider

Auditable process

Access control

Who decides permissions and privileges (‘need to know’)?

Remote access

How delivered securely?

Permit Bring Your Own Device?

Organisational – physical security

Secure Office Storage

For removable devices **and** hardcopy information

- Identifying marks?
- Kensington locks?
- Locked print?
- Offsite?

Building access control

- Secure premises – CCTV | locked windows | perimeter
- Locked CCTV room | server room
- ID badges, supervised visitors | contractors

Remote working

- Secure both hardcopies and devices when in transit.
- Kept out of sight: in transit | at home.
- Lockable pedestals | Kensington locks?

Secure disposal

- Shredding of hardcopies
- Beyond use | Reuse | Resale

Organisational – other measures

Policy, procedures, guidance & training

Eliminate ambiguities

Clearly communicated, readily accessible and understood

Human Resources

Explicit roles and responsibilities in Job Descriptions and Terms of Reference

Terms and Conditions: confidentiality clauses

Clear expectations | reporting lines

Disciplinary process

Training records

Procurement (and contracts)

i.e. outsourced services like IT and software

Due diligence

Compliant contract Terms and Conditions:

- Act on your instructions
- Equivalent security

Auditing and monitoring

Other Security Measures

- Shredding all confidential waste.
- Using strong passwords.
- Installing a firewall and virus checker on your computers.
- Encrypting any personal information held electronically.
- Disabling any ‘auto-complete’ settings.
- Holding telephone calls in private areas.
- Checking the security of storage systems.
- Keeping devices under lock and key when not in use.
- Not leaving papers and devices lying around.

12 offline measures to keep your physical data secure

- Lock rooms containing confidential information when not in use.
- Make sure employees don’t write their passwords down.
- Use swipe cards or keypads to access the office.
- Use CCTV cameras to monitor your office space.
- Shield keyboards when inputting passwords.
- Shred confidential waste.
- Use forensic property marking equipment and spray systems to mark assets.
- Use anti-climb paint on exterior walls and drains.
- Install an alarm system.
- Place bars on ground floor windows.
- Hide valuable equipment from view when not in the office.
- Assign a limited number of trustworthy employees as key safe holders.

Holding Data and Keeping it Up-to-Date

- **Carry out an information audit at least annually.**
  - Write a letter at the start of each school year asking parents and students to check that their details are correct. This also helps prevent emergency risks, e.g. if an old address or phone number is on record.
  - Check that 'live' files are accurate and up to date.
  - Any time you become aware that information needs amending, do so immediately
  - Any personal data that is out of date or no longer needed should be 'destroyed'. This may involve shredding documents or deleting computer files securely so that they cannot be retrieved.
  - Schools must follow the disposal of records schedule. This schedule states how long certain types of personal data can be held for until it must be destroyed. Some stipulations are legal obligations while others are best practice.

You are violating the Data Privacy Act if you keep any data for longer than it is needed.

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.

PERSONAL INFORMATION CONTROLLER

NAME OF THE ORGANIZATION

WEBSITE (URL) | EMAIL

COMPANY ADDRESS | TEL. NO.

HEAD OF THE ORGANIZATION

LAST NAME | EMAIL

FIRST NAME | TEL. NO.

MIDDLE INITIAL

OFFICIAL DESIGNATION (CEO/PRESIDENT)

DATA PROTECTION OFFICER

LAST NAME | EMAIL

FIRST NAME | TEL NO.

MIDDLE INITIAL | MOBILE NO.

OFFICIAL DESIGNATION | STATUS (PERMANENT: Y/N?)

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)

SUBSCRIBE 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 (MM/DD/YYYY)	

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.

PERSONAL INFORMATION CONTROLLER

NAME OF THE ORGANIZATION

WEBSITE (URL) | EMAIL

COMPANY ADDRESS | TEL. NO.

HEAD OF THE ORGANIZATION

LAST NAME | EMAIL

FIRST NAME | TEL. NO.

MIDDLE INITIAL

OFFICIAL DESIGNATION (CEO/PRESIDENT)

DATA PROTECTION OFFICER

LAST NAME | EMAIL

FIRST NAME | TEL NO.

MIDDLE INITIAL | MOBILE NO.

OFFICIAL DESIGNATION | STATUS (PERMANENT: Y/N?)

NATIONAL PRIVACY COMMISSION

Designating a DPO is the first essential step. You cannot register with the NPC unless you have a DPO.

General Qualifications

- The Data Protection Officer (DPO) should possess specialized knowledge and demonstrate reliability necessary for the performance of his or her duties and responsibilities. As such, the DPO should have expertise in relevant privacy or data protection policies and practices. He or she should have sufficient understanding of the processing operations being carried out by the Personal Information Controller (PIC) or the Personal Information Processor (PIP), including the latter's information systems, data security and/or data protection needs.

- Knowledge by the DPO of the sector or field of the PIC or PIP, and the latter's internal structure, policies, and processes is also useful.

- The minimum qualifications for a DPO shall be proportionate to his or her functions.

Duties and Responsibilities Of the DPO

a. monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:

   1. collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
   2. analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
   3. inform, advise, and issue recommendations to the PIC or PIP;
   4. ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
   5. advice the PIP or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;

NATIONAL PRIVACY COMMISSION

b. ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;

c. advice the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);

d. 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;

e. inform and 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;

NATIONAL PRIVACY COMMISSION

f. 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;

g. 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;

h. cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and

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

NATIONAL PRIVACY COMMISSION

Additional functions of a Data Protection Officer (DPO):

1. ensuring that controllers and data subjects are informed of their rights and obligations;
2. ensuring in an independent manner the internal application of the Regulation;
3. carrying out inquiries where necessary;
4. keeping a register of the processing operations carried out by the controller;
5. notifying the NPC of processing operations which may present specific risks;
6. responding to requests from NPC and cooperating with NPC

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 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

Note: In order to avoid "privilege" issues, it's not advisable to have legal counsel be the DPO.

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

In Closing: How the NPC can help

Help in delivering the message to top management

Generic guidance and frameworks (www.privacy.gov.ph)

Updates on new standards and/or circulars (www.privacy.gov.ph)

When requested, advice on specific matters (info@privacy.gov.ph)

NATIONAL PRIVACY COMMISSION

"Compliance to Data Privacy Act is not a one-shot initiative. It is a discipline and culture that must be embedded on a continuous basis within the organization."

CULTURE OF PRIVACY in the PHILIPPINES

NATIONAL PRIVACY COMMISSION

Thank you! Any questions?

info@privacy.gov.ph