Privacy Impact Assessment

Dr. Rolando R. Lansigan,
Chief, Compliance and Monitoring Division

NATIONAL PRIVACY COMMISSION

DP 14

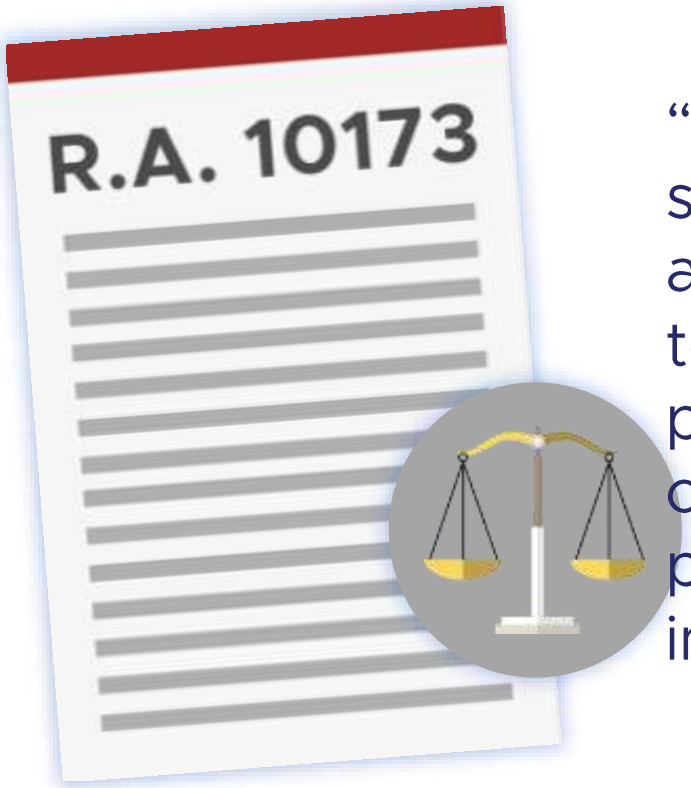
5 PILLARS OF COMPLIANCE

1	2	3	4	5
Appoint a Data Protection Officer	Conduct a Privacy Impact Assessment	Create a Privacy Management Program	Implement Data Privacy and Security Measures	Be ready in case of a Data Breach

NATIONAL PRIVACY COMMISSION

DP 14

Section 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"?

NATIONAL PRIVACY COMMISSION

DP 14

What is Privacy Impact Assessment or PIA?

NATIONAL PRIVACY COMMISSION

- What is PIA?
  - A privacy impact assessment (PIA) is a tool for identifying and assessing privacy risks throughout the development life cycle of a program or system.
  - A privacy impact assessment states what personally identifiable information (PII) is collected and explains how that information is maintained, how it will be protected and how it will be shared.
- A PIA should identify:
  - Whether the personal data being collected complies with legal requirements of the DPA
  - The risks and effects of collecting, maintaining and disseminating PII.
  - Protections and processes for handling information to alleviate any potential privacy risks.
  - Options and methods for individuals to provide consent for the collection of their PII.
- Stages of PIA
  - Stage 1: Initial Screening
  - Stage 2: PIA
  - Stage 3: Final Report and Sign Off

Pillar 2: Know Your Risks:

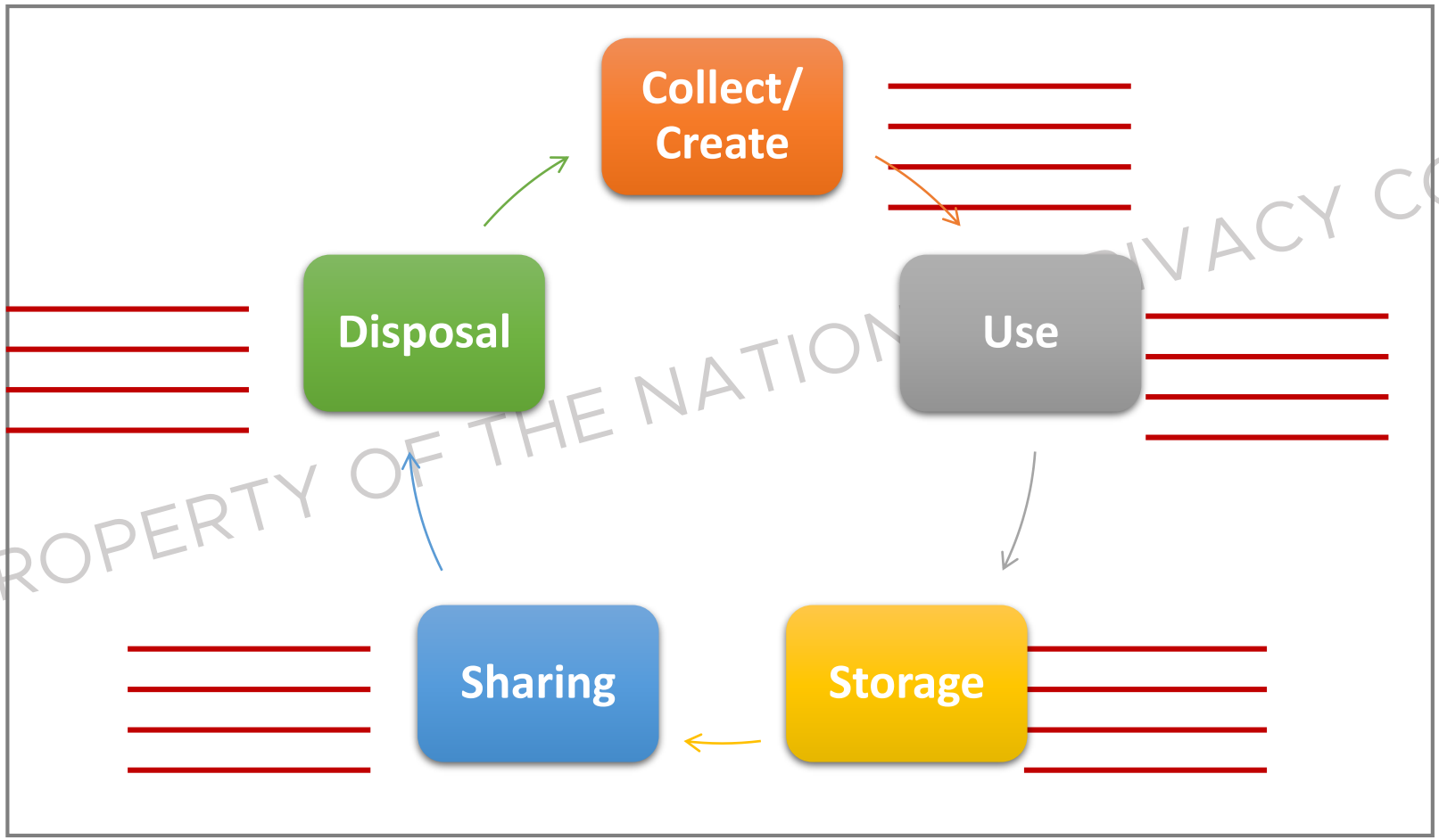
Conduct a Privacy Impact Assessment (PIA)

Legal Basis Sec. 20(c) of the DPA, Section 29 of the IRR, Sections 4-5 of Circular 16-01, 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 freedom 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 control, 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

WHO should participate in the PIA?

Those involved in the Information Life Cycle



Assign the Roles

- In your teams, assign the following roles:
  - Head of the Organization
  - Process Owner
  - Data Subject
  - Legal Officer
  - ICT Officer
  - DPO
  - Civil Society
  - HR
  - National Privacy Comm.

Sample Case Study

Vaccination Program

The Department of Health requires those who participate in the Libreng Bakuna Program to sign up using forms provided for the purpose by the DOH.

The forms indicated that the participants must enter their name, age, address, name of child, proof of billing/ residence, government-issued identification details and photo.

The sheets will be kept in a folder in the office of the Barangay Health Officer. Around one hundred families plan to avail of the free vaccination.

STAGE 1 – Initial Screening Questions

Answering "Yes" to any of the screening questions below represents a potential IG risk factor that will have to be further analyzed to ensure those risks are identified, assessed and fully mitigated.

Q	Category	Screening question	Yes/No
1.1	Identity	Will the project involve the collection of new information about individuals?	
1.2	Identity	Will the project compel individuals to provide information about themselves?	
1.3	Multiple organizations	Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?	
1.4	Data	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
1.5	Data	Does the project involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	
1.6	Data	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	
1.7	Data	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records, criminal records, or other information that people are likely to consider as private?	
1.8	Data	Will the project require you to contact individuals in ways which they may find intrusive?	

PROCESS OWNER: As the owner of this process, I have called this meeting today to conduct a privacy impact assessment. To get all of us on the same page, let us review the following:

1. What data is being collected by this process (list all, including personal as well as non-personal) 2. Which data (if any) is considered sensitive personal information (underline these)	
3. Who are we collecting this data from 4. How are we collecting this data	
5. Why is this data being collected 6. Will we use this data to make any decisions that have a legal effect on the data subject	
7. Who will be handling and accessing this data 8. Will the data be shared with any other organizations	
9. What is the key benefit/s the data subject gets from this process 10. What is the key benefit/s for the community or society	

LEGAL OFFICER: As the legal officer, I need to ensure that what we are doing is legally allowed and in compliance with the Data Privacy Act of 2012. Let us review the following:

1. What is the legal basis for collecting this data 2. Are we over-collecting	
3. How will consent be obtained 4. Do individuals have the opportunity and/or right to decline to provide data 5. What happens if they decline	
6. How will the data collected be checked for accuracy 7. How will data subjects be allowed to correct errors, if any	
8. Will the data be re-used 9. How	
10. How long are we required to keep the data 11. How do we plan to dispose of the data	

DATA SUBJECT: As one of those whose data is being collected by this process, I have certain fears and concerns about the impact of this process on my data privacy. Allow me to express these:

1. How easy would it be to identify me (on a scale of 1 to 4) if this data were to be breached or exposed?	1: virtually impossible 2: difficult but possible 3: relatively easy 4: extremely easy	
2. What things might happen if someone unauthorized gets this data 3. How might this happen (describe scenario/s) 4. How much damage would this cause me (on a scale of 1 to 4)	1: slight inconvenience 2: stressful inconvenience 3: major difficulties 4: extreme consequences	
5. What things might happen if someone alters or changes my data 6. How might this happen (describe scenario/s) 7. How much damage would this cause me (on a scale of 1 to 4)	1: slight inconvenience 2: stressful inconvenience 3: major difficulties 4: extreme consequences	
8. What things might happen if this data suddenly becomes unavailable 9. How might this happen (describe scenario/s) 10. How much damage would this cause me (on a scale of 1 to 4)	1: slight inconvenience 2: stressful inconvenience 3: major difficulties 4: extreme consequences	
11. What things might happen if this data is used for other purposes 12. How might this happen (describe scenario/s) 13. How much damage would this cause me (on a scale of 1 to 4)	1: slight inconvenience 2: stressful inconvenience 3: major difficulties 4: extreme consequences	

ICT/Developer: In order to design and implement the system properly, I need to understand the system requirements. Help me to answer the following:

The system will process personal data of Filipino nationals.			
The system will process personal data of citizens of other countries.			
The total no. of data subjects whose records we will store is more than 250.			
The total no. of data subjects whose records we will store is more than 100,000.			
We process personal data on paper and other media such as microfilm, microfiche.			
We process personal data using digital media such as hard disks, CDs, and servers.			
The personal data is used to make decisions with legal effect about the data subject.			
The personal data that we process is scattered over several geographical sites.			
The personal data will be accessed by users outside of our organization.			
The personal data will be accessed by users from other parts of the world.			
The personal data will be accessed by programs not developed by us.			
The personal data must be accessible 24 hours a day, 7 days a week.			
The data and the system can be located in the premises of a service provider.			
There is a sub-second response time requirement for access to our data.			
The number of people who will have access to the personal data is more than 50.			
The number of people who will have access to the personal data is more than 250.			
There is a high risk of natural calamity in our area.			
The data we hold is considered an attractive target for hackers and identity thieves.			
The data and the system must be kept on-premise and cannot be moved to the cloud.			
TOTAL			

Instructions

Encircle T (True), F (False), D (Don't know or not sure)

Scoring

5 points for every T
5 points for every D

Technical Risk

0 to 35: LOW
40 to 70: MEDIUM
Above 70: HIGH

DPO: As your DPO, I would like to support this process. However, allow me to ask the following questions:

		Cost/Effort (H/M/L)
Is there a way we can increase the benefits provided? If yes, how?		M
Is there a way we can collect less data and thus reduce the exposure level?		L
How can we reduce the privacy risks related to someone unauthorized getting this data?		L
How can we reduce the privacy risks related to someone altering or changing the data?		M
How can we reduce the privacy risks related to the data suddenly becoming inaccessible?		M
How can we reduce the privacy risks related to re-using the data for other purposes?		M

MAYOR/CEO/HoA: Allow me to recap the discussion so far:

Given this process	Vaccination Program
With legal purpose	DoH Regulation
Providing this benefit (H/M/L)	High
Which collects this data	name, age, address, name of child, proof of billing/ residence, government-issued ID, photo
With identification level of (1-4)	4
The privacy risks that may lead to level 3 or 4 damage are as follows	Alteration of integrity Loss of availability
Overall privacy risk (H/M/L)	High

Stage 3: Final Report and Sign Off

Identified Risks, Agreed Actions and Sign Off Form.

Privacy Issue	Risk to Individuals	Compliance Risk	Corporate Risk

What are the key privacy issues and associated compliance and corporate risks? (Some Privacy Issues may have more than one type of risk i.e. it may be a risk to individuals and a corporate risk)

Risk	Solution (s)	Result: Is the risk reduced, eliminated or accepted?

Describe the actions you could take to reduce the risk and any future steps which would be necessary (e.g. new guidance)

Risk	Approved Solution	Solution Approved by

Describe the actions you could take to reduce the risk and any future steps which would be necessary (e.g. new guidance)

Action to be taken	Date for completion	Responsibility for Action

What solutions need to be implemented?

NATIONAL PRIVACY COMMISSION

DP 14

Data Protection Officer (DPO)	
Name	
Job Title	
Signature	
Date	

Process Owner	
Name	
Job Title	
Signature	
Date	

Summary

- This is not the OFFICIAL way to do a PIA or PbD. There are many ways to do a PIA, such as a workshop, a workflow, a survey, an interview. (See ISO 29134)
- This SIMULATION is meant to show the ROLES that need to be included in a PIA, the CONCEPTS which must be considered, and the essential ELEMENTS.
- PIAs submitted to the NPC will be reviewed for: stakeholder involvement, thoroughness of risk analysis, and completeness of controls framework.
- After six months, we will also review status of controls implementation, as well as results of a breach drill for the process.

NATIONAL PRIVACY COMMISSION

DP 14

"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

DP 14

NATIONAL PRIVACY COMMISSION

Thank you! Any questions?

info@privacy.gov.ph