PRIVACY IMPACT ASSESSMENT

ATTY. VIDA ZORA G. BOCAR

ATTY. IV
COMPLIANCE AND MONITORING DIVISION

NATIONAL PRIVACY COMMISSION

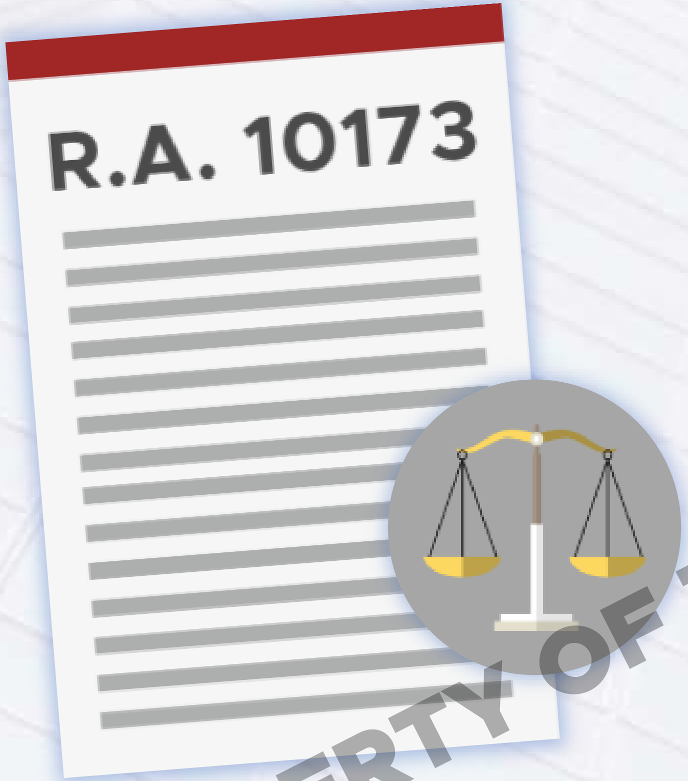
GOVERNMENT DPO CONFERENCE 2018

RULE #2

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

A **Privacy Impact Assessment** (PIA) is a process undertaken and used by a government agency to evaluate and manage the impact of its program, process and/or measure on data privacy.

DETERMINATION OF RISKS



"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." (Sec. 20, R.A. 10173)

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

DEFINITION OF PRIVACY IMPACT ASSESSMENT

"Privacy Impact Assessment" is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or PIP program, project, process, measure, system or technology product of a PIC or PIP. It takes into account the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations; (Advisory 17-03)

OBJECTIVES OF PIA (Advisory 17-03)

The PIA should identify the risks, threats and vulnerabilities of the project, program, process, measure, system or technology product within the various departments which require control measures or other interventions for personal data protection. It should determine:

a) The adherence of the PIC or PIP to the principles of **transparency, legitimate purpose and proportionality**;

b) The existing **organizational, physical and technical security measures** in the data processing systems of the PIC or PIP;

c) The extent by which the PIC or PIP **upholds rights of data subjects.**

MANAGING RISKS, LEGAL GAPS FOUND DURING PIA

The risks to privacy and data security should be addressed by a control framework, a comprehensive enumeration of the measures intended to address the risks. (also known as Privacy Management Program)

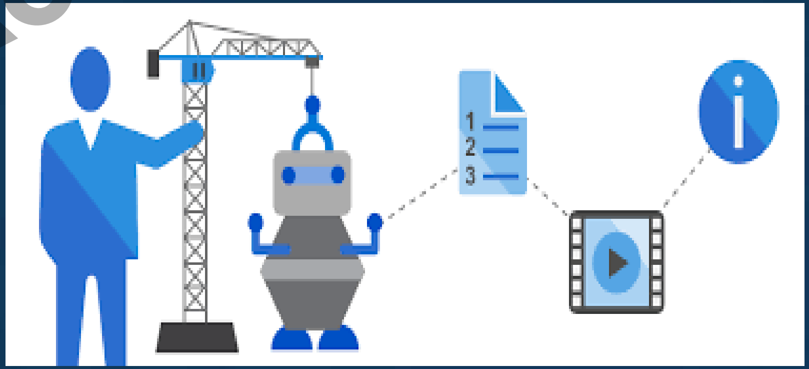
The control framework should provide measures for the protection of personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. It should also include measures to ensure that data subjects are able to exercise their rights under the Act.

When is a PIA necessary?

- Prior to setting-up of a Privacy Management Program (PMP)
- Prior to sign-off of new programs, projects, processes, measures, systems or technology products that have privacy impacts on the agency/office
- If there has been a change in the way personal data is being processed as a result of a change in law or regulation, or changes within the organization, or business expansion, merger or acquisition
- Prior to entering into a data sharing agreement with a PIC
- Prior to implementing any type of large-scale data collection
- Prior to outsourcing any type of processing to a service provider

A New or Updated PIA is also recommended in the ff. instances:

- A new or prospective technology, services or initiative where PI is or to be processed
- A decision that sensitive PI is going to be processed
- Business expansion or acquisition
- Changes in:
  - ✓ Applicable privacy-related laws and regulations,
  - ✓ Industry guidelines/professional standards;
  - ✓ Contractual obligations, internal policy;
  - ✓ Information system operations, use case content, etc



Conducting the PIA

Planning and Mobilization

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

Perform the Assessment

- Consult stakeholders, analyze risks and legal gaps, create risk map
- Determine necessary controls and remediation measures to address legal gaps and risks
- Create risk management plan, get sign off

Implement the control framework (PMP)

- Deploy risk management controls
- Adress legal gaps through remediation measures
- Monitor and evaluate on a regular basis

PIA PROCESS

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 company/agency's processes to determine whether a new/revised PIA is necessary

Program, Process, or Measure	Privacy Risk	Benefit	Controls	Impact Assessment
X.1				
X.2				
X.3				
X.4				

PRIVACY RISK is the probability that the activity involving data will result in harm, or a loss of the rights and freedoms of an individual.

CONTROLS may be applied in order to reduce severity, likelihood, and magnitude of the privacy risk

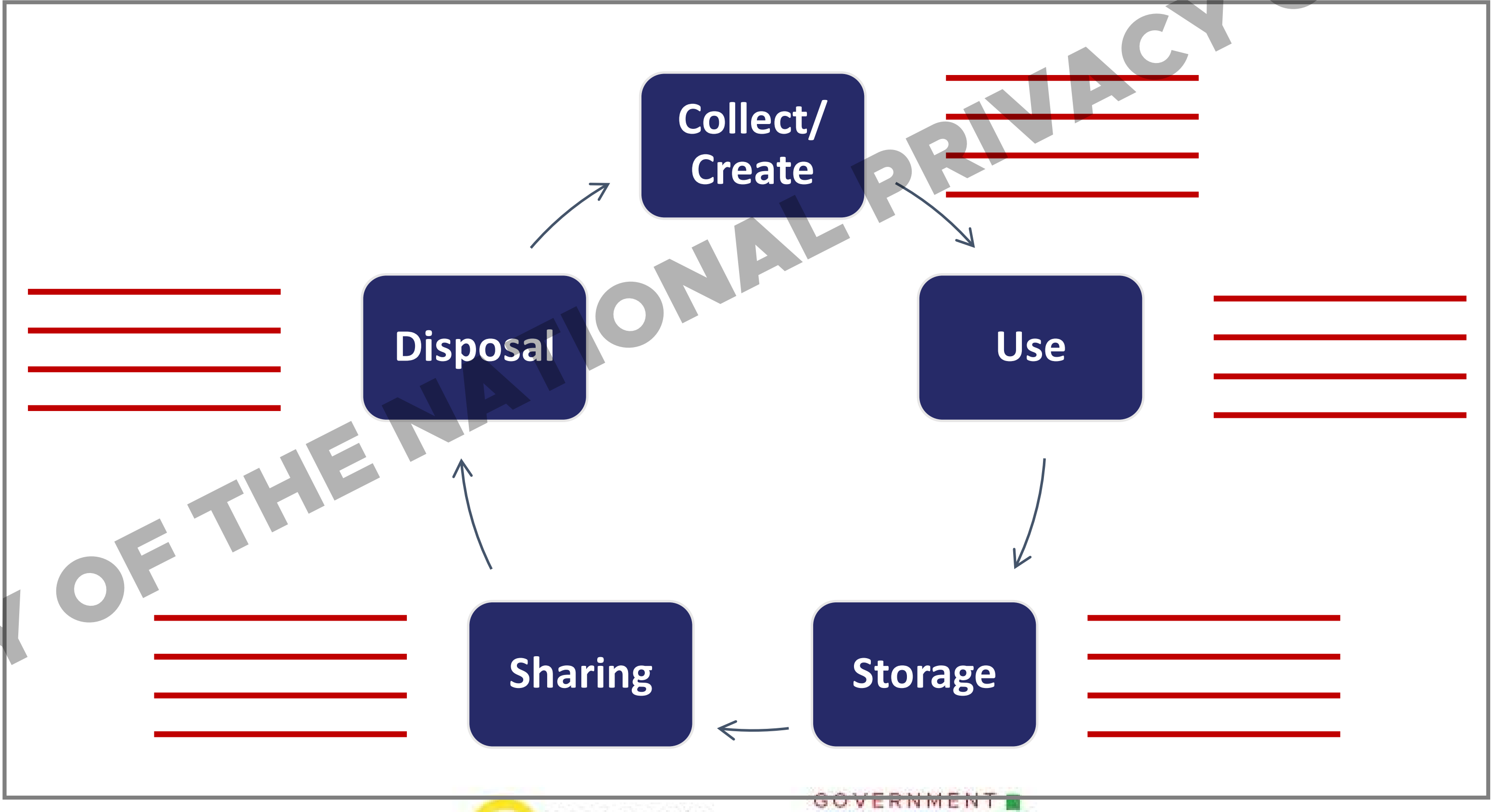
Program, Process, or Measure	Privacy Risk	Benefit	Controls	Impact Assessment
X.1	HIGH	MEDIUM		UNACCEPTABLE
X.2	HIGH	LOW	HIGH	UNREASONABLE
X.3	LOW	HIGH	LOW	ACCEPTABLE
X.4	MEDIUM	HIGH	MEDIUM	ACCEPTABLE

PIA Components

1. Ownership of System/Process
2. Stakeholder Involvement (Internal & External)
3. Privacy Risk Map/Address Legal Gaps
4. Proposal of Controls/Remediation Measures
5. Sign-off from Top Management
6. Implementation of PMP in Company/Agency

WHO should participate in the PIA?

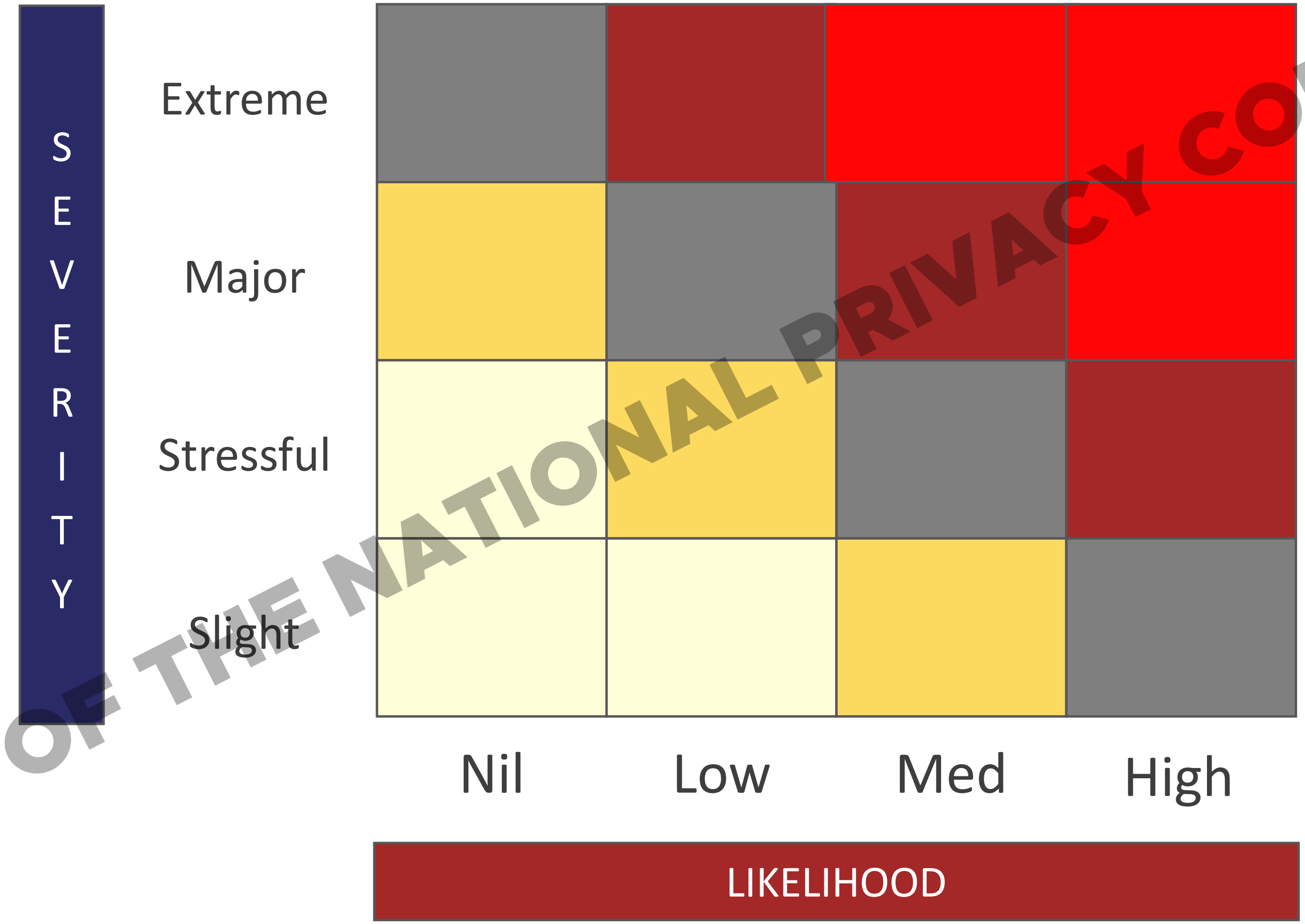
Those involved in the Information Life Cycle:



PLUS, when applicable:

- Internal stakeholders (i.e. Legal, Compliance, HR, Facilities)
- DPO/Data Protection Office/Team
- Privacy advocates

PRIVACY RISK MAP



NATIONAL PRIVACY COMMISSION

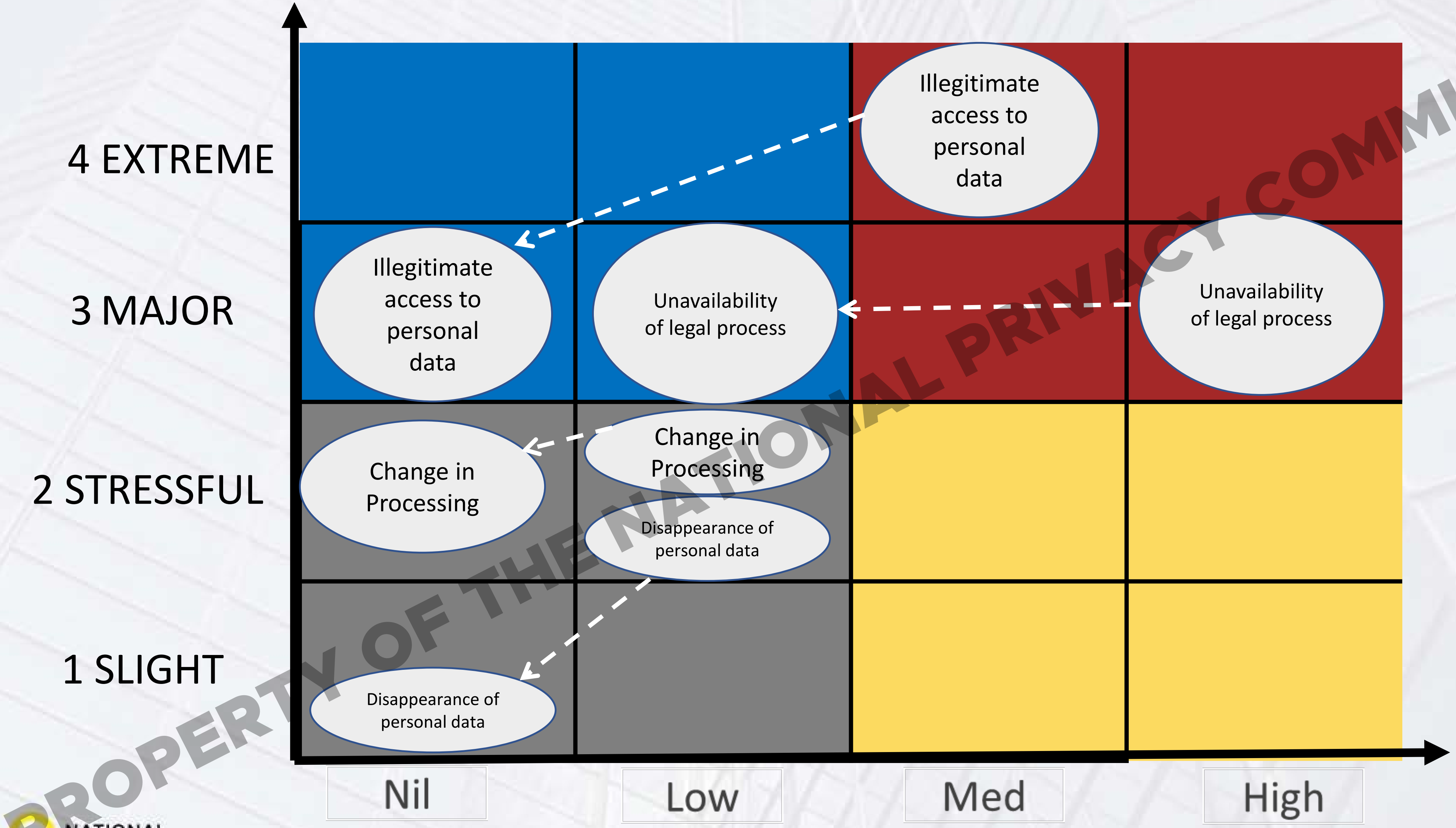
GOVERNMENT DPO CONFERENCE 2018

1. **Risk with a high severity and likelihood** absolutely must be avoided or reduced by implementing **security measures that reduce both their severity and their likelihood**. Ideally, care should even be taken to ensure that these risks are treated by independent measures of prevention (actions taken prior to a damaging event), protection (actions taken during a damaging event) and recovery (actions taken after a damaging event).

2. **Risks with a high severity but a low likelihood** must be avoided or reduced by implementing **security measures that reduce either their severity or their likelihood**. Emphasis must be placed on preventive measures.

3. **Risks with a low severity but a high likelihood** must be reduced by implementing security measures that reduce their likelihood. Emphasis must be place on recovery measures.

4. **Risks with a low severity and likelihood** may be taken, especially since the treatment of other risks should also lead to their treatment.



	Nil	Low	Med	High
4 EXTREME			Illegitimate access to personal data	
3 MAJOR	Illegitimate access to personal data	Unavailability of legal process		Unavailability of legal process
2 STRESSFUL	Change in Processing	Change in Processing Disappearance of personal data		
1 SLIGHT	Disappearance of personal data			

SAMPLE PRIVACY IMPACT ASSESSMENT

NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 2018

Case Study

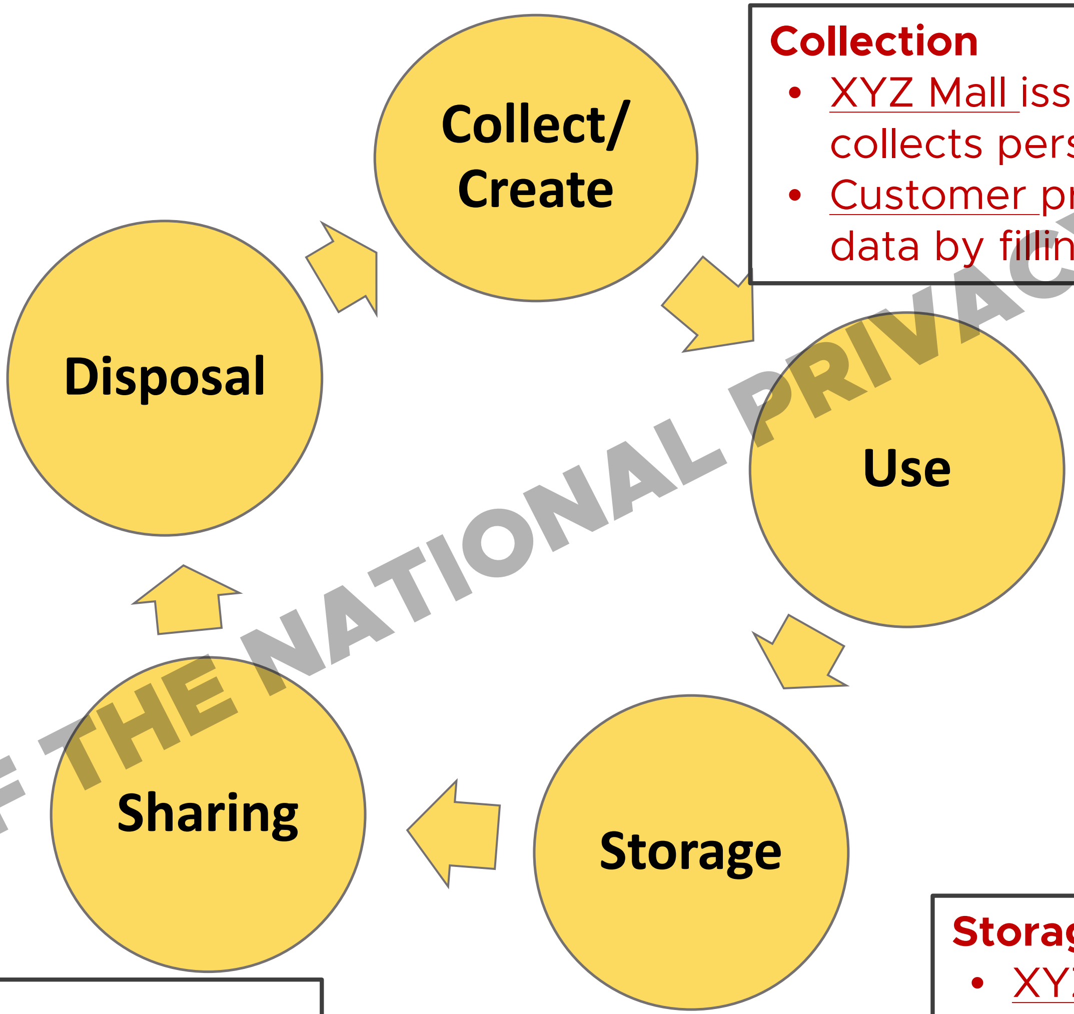
Rewards Card Program

XYZ Mall is offering a rewards program to its customers, wherein a customer is given a rewards card in which points are earned in exchange from purchases made by the customer in its participating stores and outlets. The rewards card is valid for a period of two (2) years and renewable for the same period thereafter.

A customer becomes a member by filling up an application form, either written or online, in which you list personal info such as name, address, contact number, email, date of birth, citizenship and civil status, spouse's name, all of which are required fields. A valid government ID is also required to be presented and attached along with the application form to be submitted to XYZ Mall's Customer Service Division. These personal information are stored in the company's database along with other XYZ Mall's database records.

The issuance of the rewards card is contracted out to Cards R Us, a 3rd party service provider, which has unrestricted access to the customers' application forms and attachments. M2M, a marketing research firm which tracks customers' shopping habits and preferences based on the rewards points earned by the member customers, also has access to XYZ Mall's database, as shared by XYZ Mall to better serve their customers. XYZ Mall and M2M did not execute a data sharing agreement with regards to the database.

The Information Cycle



Collection
- XYZ Mall issues form and collects personal data
- Customer provides personal data by filling up form

Use
- XYZ Mall uses data for rewards system
- Cards R Us uses data for issuance of cards
- M2M uses data for commercial marketing

Storage
- XYZ Mall stores data in its database

Sharing
- Data is shared with M2M for commercial marketing

Disposal
- Not defined

NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 2018

PIA Participants

- XYZ Mall
- Customers
- Cards R Us
- M2M Marketing

Step 1: Define the Process

1. What personal data is being collected? 2. Are we over-collecting	Name, address, contact number, email, date of birth, citizenship, civil status, spouse's name Yes – spouse's name, civil status, citizenship
3. Who are we collecting this data from 4. How are we collecting this data	Customers Application form, either written or online
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	To be issued a rewards card and be a member of the mall's rewards program
7. Who will be handling and accessing this data 8. Will the data be shared with any other organizations	Participating stores in XYZ Mall, Cards R Us employees M2M company employees
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	Discounts/preferences in participating stores and outlets Systematized discounts and rewards from participating stores

Step 2:

Ensure that processing is legally allowed and in compliance with the Data Privacy Act of 2012.

1. What is the legal basis for collecting this data 2. Are we over-collecting	Application form, either written or online Do we really need spouse's name? civil status? Citizenship?
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	Through customer filling up form and affixing signature Yes Rewards card may not be issued/certain rewards not allowed
6. How will the data collected be checked for accuracy 7. How will data subjects be allowed to correct errors, if any	Photocopy of government-issued ID; contact customer via contact details Approach customer service or email XYZ Mall
8. Will the data be re-used 9. How	Yes M2M Marketing Research for shopping preferences
10. How long are we required to keep the data 11. How do we plan to dispose of the data	During the validity of issued rewards card to customer Not indicated in the terms and conditions

Step 3:

Define the the probability that the activity involving data will result in harm, or a loss of the rights and freedoms of the data subject.

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	**4**
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	**3-4** **Hacked database/info sold to other companies** **3-4**
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	**2** **Error in encoding to database by employee** 2-3
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	**3-4** **Corrupted database/application form lost by employee**
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	**3-4** **Other malls/outlets buy personal data and engage targeted marketing**

Examples of Threats and Risks

Theft	Earthquake	Human Error
Espionage	Eavesdropping	Image Capture
Loss	Phishing	Man-in-middle
Fire	Ransomware	Forgery
Flood	DDOS	Redirection
SW Malfunction	HW Malfunction	Malice

Step 4:

Review existing controls, if any. Identify new controls using privacy-by-design principles

		Cost/Effort (H/M/L
Is there a way we can increase the benefits provided? If yes, how?	Identify additional functionality of rewards card	M
Is there a way we can collect less data and thus reduce the exposure level?	Remove spouse's name, citizenship, civil status in application form	L
How can we reduce the privacy risks related to someone unauthorized getting this data?	Issue security clearances; identify access controls	M
How can we reduce the privacy risks related to someone altering or changing the data?	Encrypt database with personal information	M-H
How can we reduce the privacy risks related to the data suddenly becoming inaccessible?	Back-up copy in separate data center	M
How can we reduce the privacy risks related to re-using the data for other purposes?	Access controls; clear outsourcing agreement	M

SEVERITY

	Nil	Low	Med	High
Extreme			Hacked/Corrupted database	Selling of database of customers' personal info
Major			Error in encoding data	Telemarketers of other stores/malls
Stressful				
Slight				

LIKELIHOOD

Step 5:

Summary (for sign-off by the “Head of Organization”)

Process	Rewards Program of XYZ Mall
Legal Purpose	Availment of Rewards and Discounts
Providing this benefit (H/M/L)	**H**
Privacy risk (H/M/L)	**H**
Controls	Organizational: Security Clearances, (**M**) Physical: Access Controls, (**M**) Technical: Back-up Copy (**M**)
Overall Assessment	Acceptable

Program, Process, or Measure	Privacy Risk	Benefit	Controls	Impact Assessment
REWARDS PROGRAM	HIGH	HIGH	MEDIUM	ACCEPTABLE

SUMMARY

- 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 DOCUMENTATION.
- 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 for guidance)
- In evaluating the risks involved in the processing, make sure to take note of the risks both to the organization and to the data subjects.
- Post-PIA: Review the status of your PMP, conduct a breach drill when applicable, and observe actual implementation of control measures.

NATIONAL
PRIVACY
COMMISSION

GOVERNMENT DPO CONFERENCE 2018

Questions?
Contact us:

Trunk line:

CMD: 517-78-10

OPC: 565-9625

or

Email us at

info@privacy.gov.ph

compliancesupport@privacy.gov.ph

Thank you!