PRIVACY IMPACT ASSESSMENT

KHANE SAMALA RAZA
PUBLIC INFORMATION & ASSISTANCE DIVISION

NATIONAL
PRIVACY
COMMISSION

Image from: https://carfromjapan.com/article/car-maintenance/drivers-not-know-brakes-system/

WHAT IS A PIA

A process to evaluate & manage impacts on personal data privacy of a PIC or PIP's program, project, process, measure, system or technology product

WHAT IS A RISK

potential of an incident to result in harm or danger to a data subject or organization

WHAT IS A CONTROL FRAMEWORK

a comprehensive enumeration of measures a PIC or PIP has established for the protection of personal data against natural & human dangers

WHY DO A PIA

A Identify, evaluate, manage & address risks through a control framework

B Assist in preparing records of processing activities & in maintaining the Privacy Management Program

WHY DO A PIA

C Facilitate compliance by determining:

- Adherence to data privacy principles
- Its existing security measures
- Extent by which data subject rights are upheld

WHEN TO UNDERTAKE

A New – prior to adoption, use or implementation

B Existing

C Changes in governing laws or regulations that may impact personal data processing

WHO SHOULD DO THE PIA

- PICs & PIPs
- May be outsourced
- DPO – must ensure; extent of involvement dependent on PIC or PIP
- Stakeholder involvement

HOW

STRUCTURE & FORM

A No prescribed standard or format

HOW

STRUCTURE & FORM

B Existing methods may be used, as long as it:

HOW

STRUCTURE & FORM

B.01 Provides a systematic description of personal data flows & processing activities of the PIC or PIP

1 Purpose of processing

2 Data inventory identifying the types of personal data

3 Sources & collection procedure

HOW

STRUCTURE & FORM

B.01

4 Functional description including info repositories

5 Personal data transfers

6 Storage & disposal method

7 Accountable & responsible persons

8 Existing organizational, physical and technical security measures

HOW

STRUCTURE & FORM

B.02 Includes an assessment of:

1 adherence to data privacy principles

2 Implementation of security measures

3 Mechanisms for exercise of data subject rights

HOW

STRUCTURE & FORM

B.03 Identifies & evaluates the risks to the rights & freedoms of data subjects, and proposes measures to address them

1 *Risk identification* – accidental loss or destruction, human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, contamination

HOW

B.03

STRUCTURE & FORM

2 *Risk evaluation* – severity or extent of impact & probability of the risk happening

3 *Remedial measures*

HOW

STRUCTURE & FORM

B.04 An inclusive process, in that it ensures the involvement of interested parties and secures inputs from the DPO and data subjects

HOW

PREPARATION

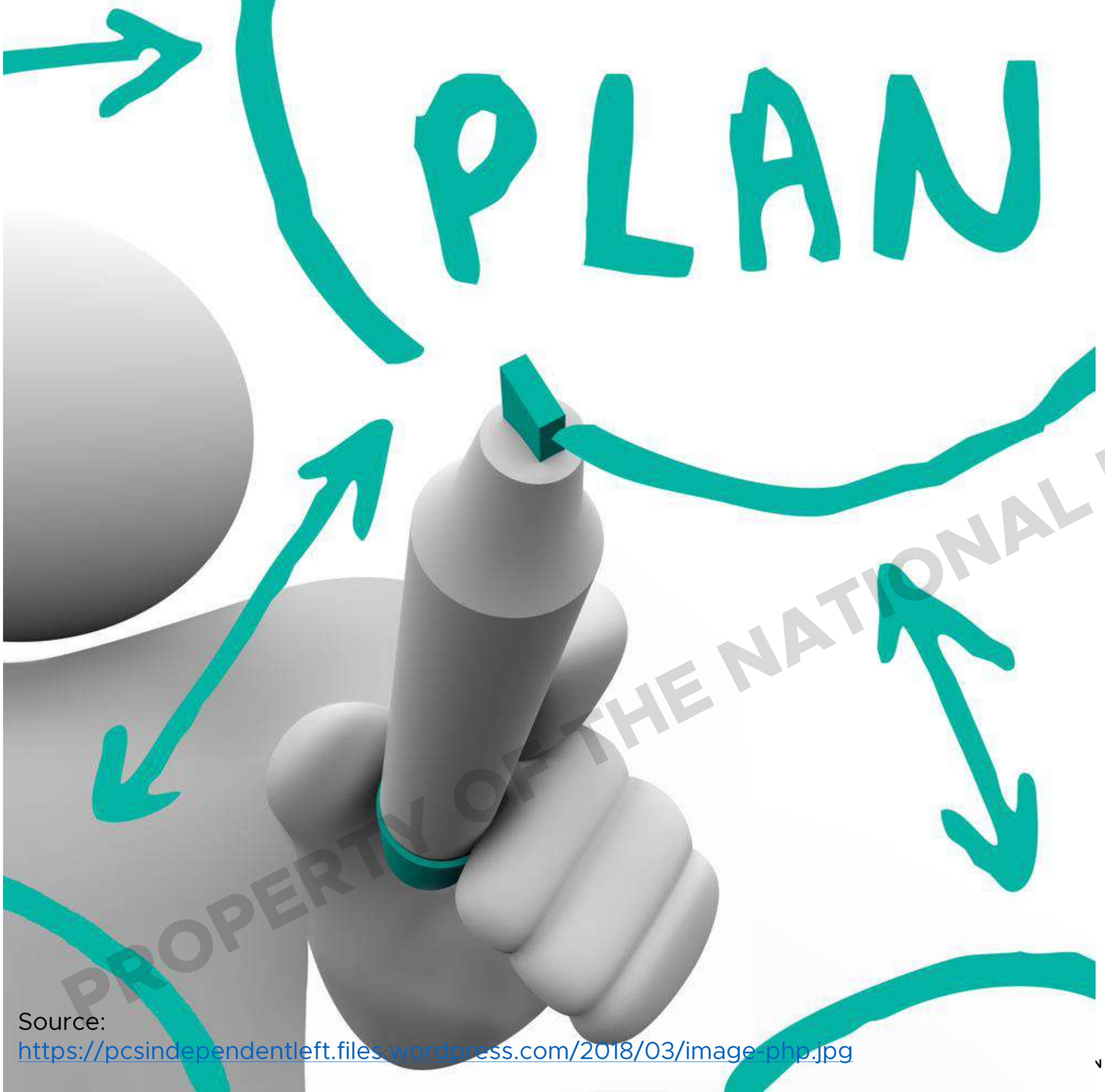
Scope

Objectives

Methodology

Control framework

Image source: http://it-one.co.ao/en/methodology/



Source:
https://pcsindependentleft.files.wordpress.com/2018/03/image-php.jpg

1 Schedule & timeline

2 Approval of resource allocation

3 Participant & methods – stakeholders

4 Documentation & review process

STAKEHOLDER CONSULTATION

Image source: https://www.toolshero.com/project-management/stakeholder-management/

PERSONAL DATA FLOWS

Collection	Storage & Transfer	Use	Retention	Disposal & Destruction
Receive application via: - careers site - application via email				
	Application stored on: - careers site - applicant tracking system (ATS)			
		HR evaluates applicant based on submission		
		If yes, administer exam	If no, notify of rejection & retain data in ATS for 3 months	Shred physical copy. Purge electronic copy.

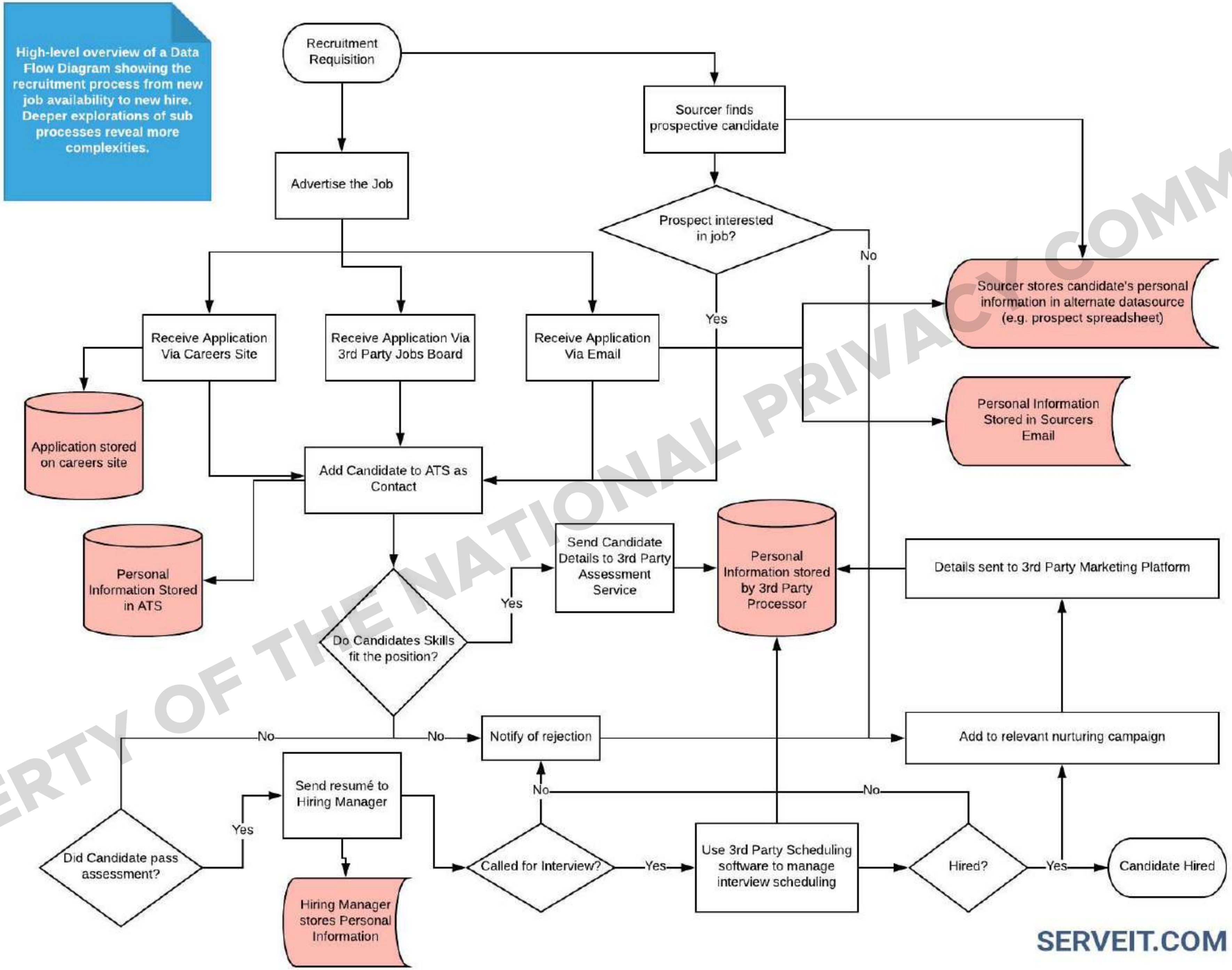
PERSONAL DATA FLOWS

Collection	Storage & Transfer	Use	Retention	Disposal & Destruction
		HR administers exam		
		If applicant passes the exam, send application & exam results to Hiring Manager	If applicant fails the exam, notify of rejection & retain data in ATS for 3 months	Shred physical copy. Purge electronic copy.
	Hiring Manager stores application			
		Hiring Manager decides on whether to call applicant for interview		
		If yes, administer	If no, notify of	Shred physical

PERSONAL DATA FLOWS

Collection	Storage & Transfer	Use	Retention	Disposal & Destruction
		If yes, administer interview	If no, notify of rejection & retain data in ATS for 3 months	Shred physical copy. Purge electronic copy.
		Recruitment & Selection Board interviews & evaluates applicant		
		If applicant is hired, process documents	If applicant is not hired, notify of rejection & retain data in ATS for 3 months	Shred physical copy. Purge electronic copy.

High-level overview of a Data Flow Diagram showing the recruitment process from new job availability to new hire. Deeper explorations of sub processes reveal more complexities.



Recruitment Requisition

Sourcer finds prospective candidate

Advertise the Job

Prospect interested in job?

No

Yes

Sourcer stores candidate's personal information in alternate datasource (e.g. prospect spreadsheet)

Receive Application Via Careers Site

Receive Application Via 3rd Party Jobs Board

Receive Application Via Email

Personal Information Stored in Sourcers Email

Application stored on careers site

Add Candidate to ATS as Contact

Personal Information Stored in ATS

Send Candidate Details to 3rd Party Assessment Service

Personal Information stored by 3rd Party Processor

Details sent to 3rd Party Marketing Platform

Yes

Do Candidates Skills fit the position?

No

No

Notify of rejection

Add to relevant nurturing campaign

Send resumé to Hiring Manager

No

No

Yes

Did Candidate pass assessment?

Called for Interview?

Yes

Use 3rd Party Scheduling software to manage interview scheduling

Hired?

Yes

Candidate Hired

Hiring Manager stores Personal Information

SERVEIT.COM

PRELIM ASSESSMENT OF BASELINE INFO

HOW

CONDUCT

USING THE BASELINE INFO & OTHER DOCS:

- evaluate processing activities against the legal obligations, and the latter's chosen control framework
- check adherence to data privacy principles, existence of planned and on-going security measures, and mechanisms for exercise of data subject rights
- determine any gaps at any stage of the processing

USING THE BASELINE INFO & OTHER DOCS:

- assess risks & identify measures to address them
- document stakeholder involvement
- review report
- submit report to management and communicate to internal & external stakeholders

EXERCISE

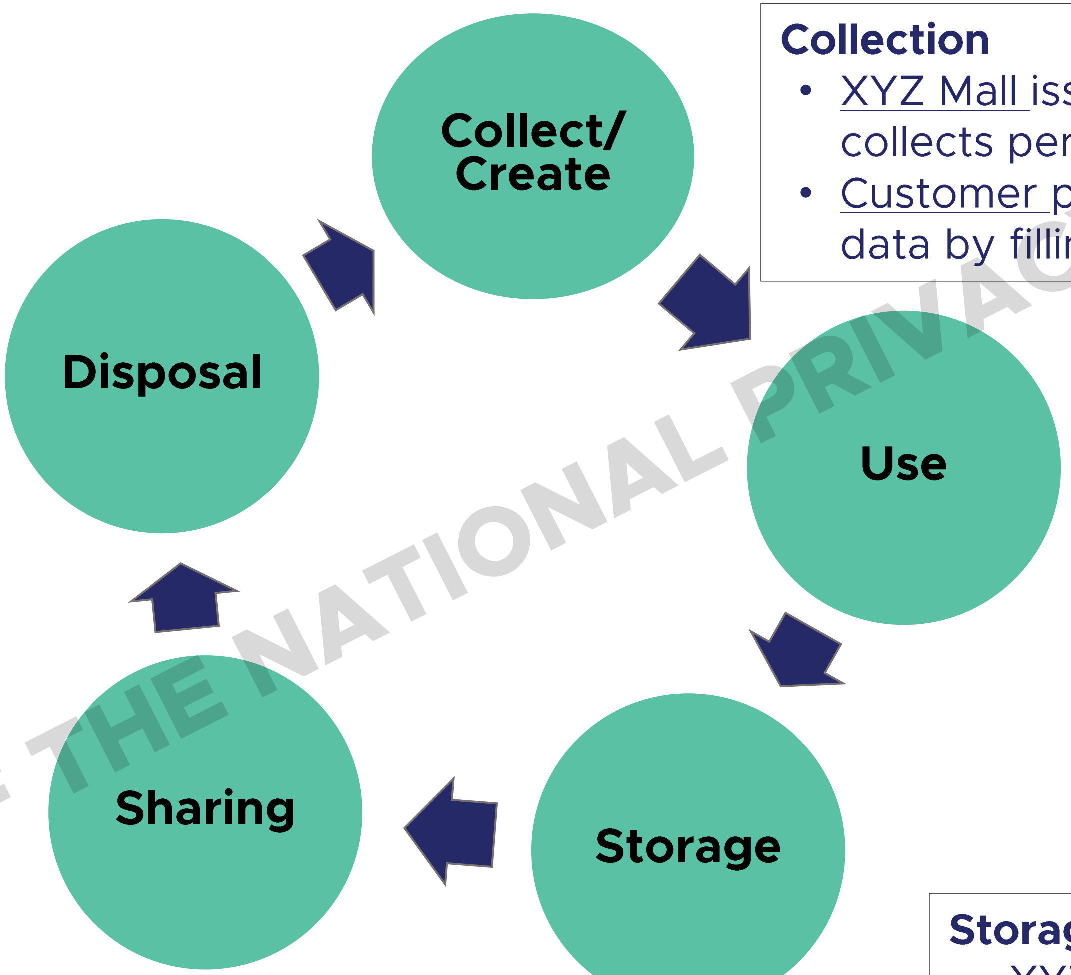
REWARDS CARD PROGRAM

XYZ Mall offers a rewards program to its customers, wherein a customer is given a rewards card that earns points for every purchase made by the customer in its participating stores and outlets. The rewards card is valid for 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 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

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

Impact		
Rating	Types	Description
1	Negligible	The data subjects will either not be affected or may encounter a few inconveniences, which they will overcome without any problem.
2	Limited	The data subject may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.
3	Significant	The data subjects may encounter significant inconveniences, which they should be able to overcome but with serious difficulties.
4	Maximum	The data subjects may encounter significant inconveniences, or even irreversible, consequences, which they may not overcome.
Probability		
1	Unlikely	Not expected, but there is a slight possibility it may occur at some time.
2	Possible	Casual occurrence. It might happen at some time.
3	Likely	Frequent occurrence. There is a strong possibility that it might occur.
4	Almost Certain	Very likely. It is expected to occur in most circumstances.

STEP 3:
ASSESS RISKS

Guide Questions	Remarks	I	P	Risk Rating
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	4	16
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	- Hackers/fraudsters can cash out reward points, use points to buy merchandise, use credentials to access other accounts including financial ones - Exploiting vulnerabilities in retailer's platform, compiling info from 3rd party sites	3-4	3-4	9-16
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	- Reward points not earned, poor customer experience if hacker was able to manipulate sales figures - Encoding error, exploiting vulnerabilities in retailer's platform, (un)intentional misconfiguration by 3rd parties	2	3-4	6-8
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	- Reward points not earned, poor customer experience - Corrupted database, (un)intentional misconfiguration by 3rd parties	2-3	3-4	6-12
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	- Fooled into spending on things you don't really need, changes in member's behavior as consumer according to retailer's schedule, without member's knowledge & consent - Data sold to other entities	3-4	3-4	9-16

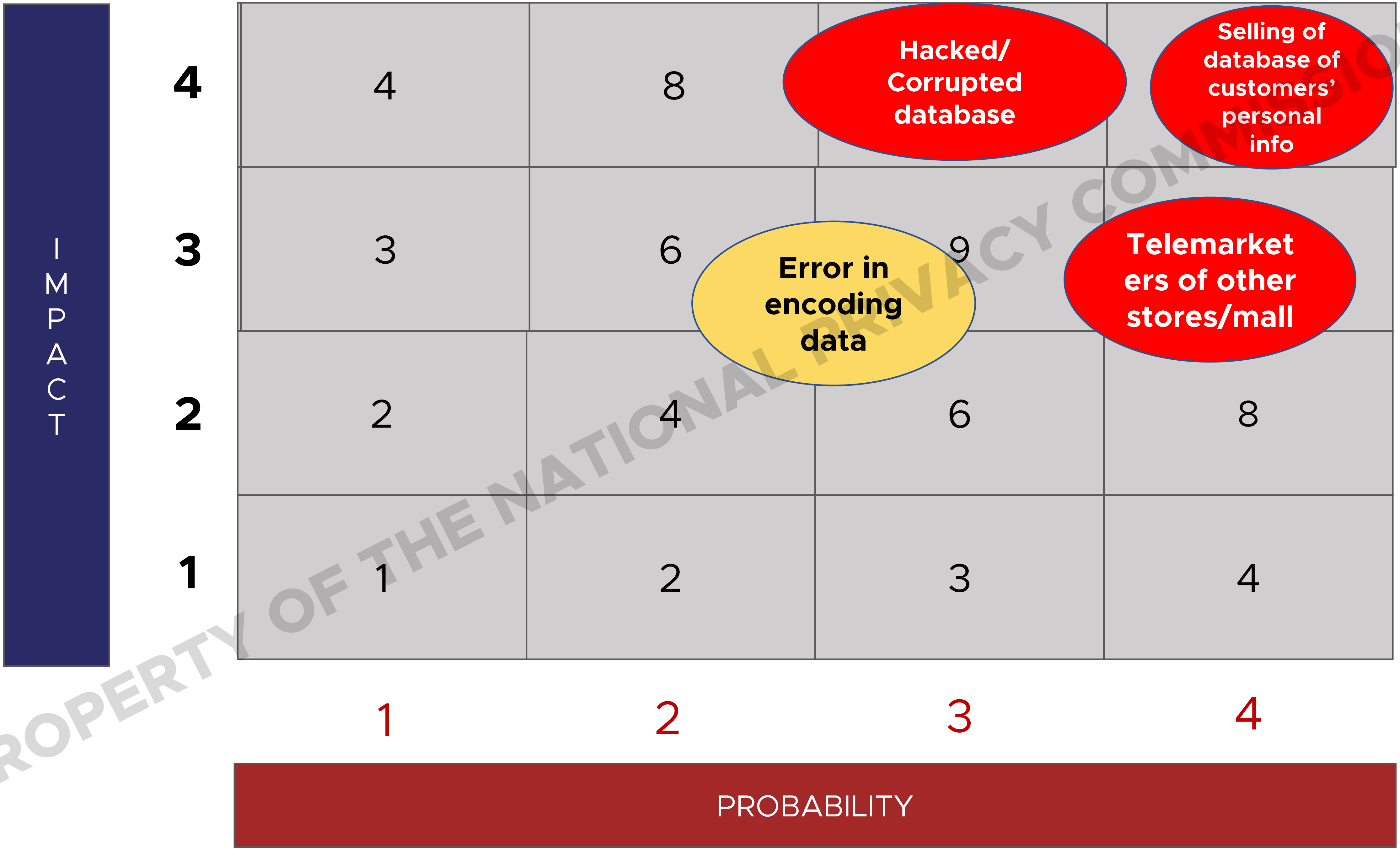
EXAMPLES OF THREATS AND RISKS

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

Guide Questions	Controls	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 & DSA	M



IMPACT				
4	4	8	Hacked/ Corrupted database	Selling of database of customers' personal info
3	3	6	9 Error in encoding data	Telemarketers of other stores/mall
2	2	4	6	8
1	1	2	3	4
	1	2	3	4

PROBABILITY

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/N)	**13.6 = 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.

NOW, IT'S YOUR TURN!

NATIONAL
PRIVACY
COMMISSION

✉ info@privacy.gov.ph

privacy.gov.ph

☎ 0939 963 8715
0945 1534 299