National Privacy Commission

Privacy Impact Assessment (Template)

Part 1 – General Description

Name of Organisation:			
Name of Program, Process or Measure:			
Date:			
PIA Drafter:			
Email:		Phone:	
Program Manager:			
Email:		Phone:	

[For the rest of the document, please delete the italicised descriptive text and, when necessary, replace it with your own.]

1. Description of Program, Process or Measure involving personal data

This section should provide a description of the program, process or measure and the context in which it functions, including: the purpose of the program and how it functions, its expected benefits, any other process or program (if any) of which it is a part, the legal authority the organisation has to implement the program, all other parties involved and the roles they play, including a description of all contracted service providers (CSPs)

2. Scope of this PIA and any Related Privacy Impact Assessments

This section should explain, what part or phase of the program the PIA covers and, where necessary for clarity, what it does not cover. This section should also identify, where applicable, any PIAs for other parts of the program that have already been completed or that will be undertaken at a later date. Please also identify if you have any public interest determinations, information usage arrangements or certifications in place under the PDPA related to this program.

The PIA should consider compliance with privacy obligations from the perspective of the organisation completing it. Where more than one organisation is involved, each party should undertake a PIA with respect to its own obligations and authorities. If multiple organisations decide to complete a joint PIA, separate privacy assessments will need to be undertaken for each party. In this case the PIA should clearly distinguish between the assessments for each organisation.

Part 2 – Threshold Analysis

The threshold analysis will be in two parts. The firs is the identification of personal information that is currently or will be used in the project.

The program will collect, use, retain, disclose, dispose the following personal Information.
(Please check the appropriate box)

	Personal Information	**Y**	**N**
1	Name		
2	Home Address		
3	Business Address		
4	Email Address		
5	Telephone Number - Work		
6	Telephone Number - Home		
7	Age		
8	Date of Birth		
9	Marital Status		
10	Color, Race or Ethnic Origin		
11	Religion (Religious beliefs or affiliations)		
12	Education		
13	Photo		
14	Biometrics		
15	Political Association		
15	Philosophical Beliefs/Orientation		
16	Health		

17	Sexual life/preference/practice		
18	Offence committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings		
19	Issued by government agencies peculiar to an individual • unique identifiers (eg TIN, UMID ID no., Driver's License no, Passport no, GSIS/SSS number, Voter's Registration no, etc) • previous or current health records • licenses or its denials, suspension or revocation • tax returns		
20	Specifically established by an executive order or an act of Congress to be kept classified		
21	Others, please add as many as will be collected		

Please respond to the following questions and provide explanations/comments if necessary

	Y/N	Explanation/Comments
Will the project involve the collection of new information about individuals?		
Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?		
Will you be using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		
Will the initiative require you to contact individuals in ways which they may find intrusive?		
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		
Does the initiative involve you using new technology		

which might be perceived as being privacy intrusive e.g. biometrics or facial recognition?		
Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		

If this program will **not** collect, use or disclose any of the above information, please proceed to Part 5 – Summary of Assessment and Sign Off

N.B. Not using personal information, when warranted, can also raise potential risks. Please make sure that you are not sim[ly trying to avoid doing a full-blown PIA when you declare that the project is not using personal information.

Part 3. Stakeholder Engagement

The following stakeholders were consulted for this PIA

Please identify all project stakeholders (persons or organizations that can affect, be affected by, or perceive themselves to be affected by a decision or activity – ISO/Guide 73:2009) in the table below.

Internal Stakeholders	External Stakeholders
1	1
2	2
3	3
4	4

The stakeholders were engaged in the following manner.

Describe how stakeholders were engaged in the PIA process.

Part 4 – Data Privacy Analysis

3.1 Information Flow Description and Table

Table below describes the information flow of the project.

Describe the information flow by answering the following key questions:

- *What personal information is currently being collected and used?*
- *How does it flow through the agency or organization's systems?*
- *How will the proposed system or project change the information flow?*
- *What are the changes to personal information involved in the project? For instance:*
  - *Is new personal information being collected? If so, whom is it being collected from?*
  - *If the project involves information the organization already holds, will it be used for a different purpose? If so, why and how?*
  - *What measures are in place to ensure the information is accurate and up to date?*
  - *Will the agency or organization tell the individuals what their information will be used for? If so, how?*
  - *Who will have access to the information within the agency or organization? Who will have access to it outside the agency or organization?*
  - *How long will the information be kept? How will it be disposed?*

Table 3: Information Flow

Personal Information	**Collect** by? from? how? when? where why? authority?	**Use** by? how? when? where? why?	**Retain** by? how? how long? where? why?	**Disclose** by? to? how? when? where why? authority?	**Dispose** by? how? when? where? why? authority?
1					

2					
3					
4					

As an alternative you may use a diagram to illustrate the information flow.

3.2 Compliance with Information Privacy Principles

Each program, project or means for collecting personal information should be tested for consistency with the following Data Privacy Principles (as identified in Rule IV, Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012").

Transparency		Yes	No
1	Are data subjects aware of the nature, purpose, and extent of the processing of his or her personal data?		
2	Are data subjects aware of the risks and safeguards involved in the processing of his or her personal data?		
3	Are data subjects aware of his or her rights as a data subject and how these can be exercised?		
4	Is there a document available for public review that sets out the policies for the management of personal information? *Please identify document(s) and provide link where available* _____ _____		
5	Are there steps in place to allow an individual to know what personal information it holds about them and for what purposes it collects, uses and discloses it?		
Legitimate Purpose		Yes	No

1	Is the processing of personal information compatible with a declared and specified purpose which are not contrary to law, morals, or public policy?		
Proportionality		Yes	No
1	Is the processing of personal information • adequate, • relevant, • suitable, • necessary, and • not excessive in relation to a declared and specified purpose?		
2	Is personal information being processed because the purpose of the processing could not be reasonably fulfilled by other means?		

Collection		Yes	No
1	Is the collection of personal information for a declare, specified and legitimate purpose?		
2	Is individual consent secured prior to the collection and processing of personal data?		
3	Is consent time-bound in relation to the declared, specified and legitimate purpose?		
4	Can consent be withdrawn?		
5	Is all the information collected necessary for the program?		
6	Is it not possible for the individual to remain anonymous for the purpose of the program?		
7	Is the information being collected directly from the individual?		
8	Will any information also be collected indirectly about the individual?		
9	Will this program assign or collect unique identifiers?		
10	Is it necessary to assign a unique identifier to individuals to enable your organisation to carry out the program?		
11	Will a unique identifier of another agency be used?		

Use and Disclosure		Yes	No
1	Personal information will only be used or disclosed for the primary purpose identified?		
2	Personal information will also be used or disclosed for a secondary purpose?		
3	If using personal information for a secondary purpose, which of the following applies? • The individual has consented to the use or disclosure • The secondary purpose is related to the primary purpose, • The individual would reasonably expect the organisation to use or disclose the information for the secondary purpose • Necessary for research, or the compilation or analysis of statistics in the public interest. If yes, please explain _____ _____ _____ • To lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare; • To lessen a serious threat to public health, public safety or public welfare • On suspicion or unlawful activity as part of reporting its concerns to relevant persons or authorities • As required or authorised by law *Please site the relevant law:* _____		
Use and Disclosure of a Unique Identifier given by another organization		Yes	No
1	Will this program use or disclose a unique identifier assigned to an individual by another organisation?		
2	The unique identifier assigned to an individual <u>by another organisation</u> will be used and/or disclosed only when: • The individual has consented • It is necessary for the organisation to fulfil its obligation to the other organisation • A serious threat to individual or public health, safety or welfare • Upon the request of a government agency to monitor unlawful activity or as part of an investigation • It is required or authorised by law ▪ *If YES, please site the relevant law:* _____ _____		
Data Quality		Yes	No
1	Please identify all steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date.		

	• information was obtained from a reputable source such as another government agency, • the system is regularly tested for accuracy, • periodic reviews of the information, • a retention schedule in place that deletes information that is over a certain period; • staff are trained in the use of the tools and receive periodic updates, • reviews of audit trails are undertaken regularly, • independent oversight, • incidents are reviewed for lessons learnt and systems / processes updated appropriately. • *Others, please specify* _____ _____		
Data Security		Yes	No
1	The program has taken reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure?		
2	If yes, which of the following has the program undertaken to protect personal information across the information lifecycle: • identifying and understanding information types • assessing and determining the value of the information • identifying the security risks to the information • applying security measures to protect the information • managing the information risks.		
Records Management		Yes	No
1	The program will take reasonable steps to destroy or de-identify personal information if it is no longer needed for any purpose. *If YES, please list the steps* _____ _____		

Cross-border Data Flows (optional)		Yes	No
1	The program will transfer personal information to an organisation or person outside of the Philippines *If YES, please describe:* _____ _____ _____		

2	Personal information will only be transferred to someone outside of the Philippines if any of the following apply: • The individual consents to the transfer • The organisation reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to the DPA of 2012 • The transfer is necessary for the performance of a contract between the individual and the organisation • The transfer is necessary as part of a contract in the interest of the individual between the organisation and a third party • The transfer is for the benefit of the individual; • It is impractical to obtain consent; • If it were practicable the individual would likely consent.		
3	The organisation has taken reasonable steps so that the information transferred will be held, used and disclosed consistently with the DPA of 2012 *If YES, please describe steps:*		

Part 4 – Privacy Risk Management

For the purpose of this section, a risk is something that could lead to the unauthorised collection, use, disclosure or access to personal information.

The first step in managing risks is to identify them by identifying threats and vulnerabilities and evaluating Impact and likelihood and providing a risk rating for each phase of the information life cycle.

The following definitions are used in this section,

Threat – "a potential cause of an unwanted incident, which may result in harm to a system or organization";

Vulnerability – "a weakness of an asset or group of assets that can be exploited by one or more threats";

Likelihood - chance or probability of something happening;

Impact - severity of the injuries that might arise if the event does occur (can be ranked from trivial injuries to major injuries); and

Risk Rating – a function of the probability and impact of an event

For further reading/guidance, please consult the following:

- ISO/Guide 73:2009(en) Risk management — Vocabulary *https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en*
- *Information and Privacy Commissioner, Ontario, Canada, "Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default " https://www.ipc.on.ca/wp-content/uploads/2010/04/Privacy-Risk-Management-Building-privacy-protection-into-a-Risk-Management-Framework-to-ensure-that-privacy-risks-are-managed.pdf*
- *CNIL "Managing Privacy Risks Assessment Methodology" https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf*
- *European Network and Information Security Agency (ENISA), "Risk Management" https://www.enisa.europa.eu/topics/threat-risk-management/risk-management?tab=details*

	Threats	**Vulnerabilities**	**Impact**	**Likelihood**	**Risk Rating**
Collection	1				
	2				
Use	1				
	2				
Retention	1				

	2				
Disclosure/ Data Sharing	1				
	2				
Disposal	1				
	2				

The next step is Risk Treatment or the process of selection and implementation of measures to modify risk.

Common risk treatment measures include:

- *Avoid / Eliminate – stop or remove the activity or situation that could cause the risk to occur.*
- *Mitigate – introduce or modify existing controls that may reduce the consequence or likelihood of the risk.*
- *Accept – agree to accept the risk and its consequences.*

From the risks identified in the previous section, list existing controls to treat the risks, if any, identify proposed mitigation measures

Risks - General	**Risk Rating**	**Existing Controls**	**Proposed Mitigation Measures (justification)**
1			
2			
Risks - Collection	**Risk Rating**	**Existing Controls**	**Proposed Mitigation Measure (justification)**
1			
2			
Risks - Use	**Risk Rating**	**Existing Controls**	**Proposed Mitigation Measures (justification)**

1			
2			
Risks - Retention	**Risk Rating**	**Existing Controls**	**Proposed Mitigation Measures (justification)**
1			
2			
Risks – Disclosure/ Data Sharing	**Risk Rating**	**Existing Controls**	**Proposed Mitigation Measures (justification)**
1			
2			
Risks - Disposal	**Risk Rating (H/M/L)**	**Existing Controls**	**Proposed Mitigation Measure (justification)**
1			
2			

Part 5 – Summary of Assessment and Sign Off

Summary

Insert a summary or overview of the most significant findings in relation to both identified privacy risks and identified privacy-enhancing features. Where appropriate also include critical recommendations. The summary should include an overview of which privacy risks cannot be mitigated, the likely public reaction to such risks, and whether the risks are outweighed by the public benefit in the project proceeding.

Signatures

Program/Process Owner	Signature	Date
Data Protection Office	Signature	Date