PRIVACY MANAGEMENT PROGRAM

MR. JONATHAN RUDOLPH Y. RAGSAG
Data Security and Technology Standards Division
National Privacy Commission

NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 2018

5 PILLARS OF COMPLIANCE

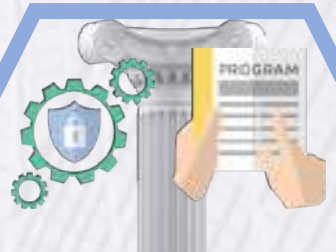
1

Commit to Comply:
APPOINT A DATA PROTECTION OFFICER

2

Know Your Risks:
CONDUCT A PRIVACY RISK OR IMPACT ASSESSMENT

3



Write Your Plan:
CREATE A PRIVACY MANAGEMENT PROGRAM

4

Be Accountable:
IMPLEMENT YOUR PRIVACY AND DATA PROTECTION MEASURES

5

Be Prepared for Breach:
REGULARLY EXERCISE YOUR BREACH REPORTING PROCEDURE

NATIONAL PRIVACY COMMISSION

Government DPO Conference 2018

GOVERNMENT DPO CONFERENCE 2018

With the passage of Republic Act (RA) No. 10173 otherwise known as the Data Privacy Act (DPA) of 2012, government and private organizations covered by the DPA – or the Personal Information Controllers (PICs) and Personal Information Processors (PIPs) – are asking **how** do they start complying with the law. The simple answer is to have a **PRIVACY MANAGEMENT PROGRAM (PMP)** in place.

A PMP will lead organizations, both in the public and private sectors, toward a ***culture protective of data privacy rights of individuals as part of their corporate governance responsibilities***.

Privacy Management Program (PMP)

A PMP is a **holistic approach** to **privacy and data protection**, important for all agencies, companies or other organization involved in **processing of personal data**.

It minimizes the **risks of privacy breaches**, **maximizes the ability to address underlying problems**, and **reduces the damage arising from breaches**.

Demonstrates commitment to building trust with employees and clients through open and transparent information policies and practices.

Importance of a PMP

❑It puts everyone on the same page.

- A PMP provides an easier way to explain to the management and staff:
  - ✓ why is the organization doing this;
  - ✓ what are the results we expect;
  - ✓ what are the benefits of those results
  - ✓ what do organizations need to do to get there.
  - ❖ This will ensure that everyone are on board.

❑Compliance with the Act becomes more manageable.

- A PMP reduces the likelihood that organizations will violate the law, its IRR, NPC Circulars and Advisories and all other Commission issuances as it outlines the WHATs and HOWs of data privacy.

Importance of a PMP

❑ **It gives PICs and PIPs competitive advantage.**

- Implementing a PMP shows your organization's commitment to protect the personal information of your customers and clientele. This will, in turn, lead to increased trust and higher patronage.

❑ **It saves PICs and PIPs from avoidable expenses.**

- A strong and robust PMP can lead to prevention of "clean-up costs" brought about by personal data breaches. Further, it helps safeguard the reputation of organizations and individuals as well.

KEY COMPONENTS

- ORGANIZATIONAL COMMITMENT
- PROGRAM CONTROLS
- CONTINUING ASSESSMENT and REVISION

ORGANIZATIONAL COMMITMENT

Management Buy-In

- Top management support is a pivotal key to a successful writing of a PMP and essential for the emergence of a culture of privacy in the PIC or PIP.
- This means Management must:

1. Designate a Data Protection Officer (DPO) or a Compliance Officer for Privacy (COP) as the case may be;
2. Endorse a set of Program Controls; and
3. Report to the Board, as appropriate, on the program

Accountable and Responsible Persons

- The **Data Protection Officer (DPO)** is entrusted to manage the privacy management program.
- He shall be responsible in ensuring compliance with the law (RA 10173), its Implementing Rules and Regulations (IRR), Circulars and Advisories and all other Commission issuances relating to data privacy and protection.
- Must be independent and with a significant degree of autonomy in performing his/her duties.
- **May perform other duties or assume other functions as long as it will not create conflict of interest.**

See: NPC Advisory 17-01 (Designation of Data Protection Officers)

Reporting Mechanisms

- Establish internal reporting mechanisms to ensure that the PMP is structured and whether it is functioning as expected.

TOP MANAGEMENT → BOARD OF DIRECTORS

- PICs and PIPs should establish internal audit and assurance program to monitor compliance with personal data protection policies which can take the form of customer/citizen and employee feedback (for small organizations) and third-party verifications (for large organizations).

Characteristics of an effective reporting program:

1. clearly defines its reporting structure (in terms of reporting on its overall compliance activities) as well as employee reporting structures in case of complaints or a potential breach

2. tests and reports on the results of its internal reporting structures; and

3. documents all its reporting structures.

PROGRAM CONTROLS

Records of Processing Activities

- PICs and PIPs should know:
  i. what kinds of data it holds
  ii. how the personal data is being used
  iii. whether or not the PIC or PIP really need those data.

- Knowing, understanding and documenting all these things is important as this will:
  - affect the type of CONSENT the PIC or PIP needs to obtain from its Data Subjects
  - the manner on how the data is to be protected
  - make easier to assist individuals in exercising their data access and correction rights

Example of a personal data inventory

WHY	WHO	WHAT			WHEN				WHERE
		Type	Source	Legal basis	Originally	Updated	Retention period	Determined by:	
STAFF ADMIN	Current staff member	Name	Individual	Contract	Appointment	As required	Staff records retained for 6 yrs after termination unless ongoing litigation	Employment/ limitation law	Manual records - HR department/Spreadsheet held on Cloud server located IOM
		Address				As required			
		Contact details				Regularly			
		Health details				As required			
		CV			Pre-appointment	No			
		References	third party		Pre-appointment	No			
		CRB check	third party		?	?	Copy not retained, record of number only	CRB Code of Practice	
		Passport details	Individual	**Not sure - find out**	?	?	?	?	
		Work permit	individual/ third party		?	?	?	?	
		Appraisals	Individual	Legitimate interests - staff management	Annually	Regularly	3yrs after completion	Standard practice	
		Annual leave			At request	As required	**? Not sure - find out**		
		Disciplinary	individual/ third party		At the time	As required	**? Not sure - find out**		
		Tax/NI	individual/ third party			As required	**? Not sure - find out**	Tax law	**IOM Payroll company - not sure where data is held??**
		Bank account	individual	Contract	Appointment	As required			
		Pension details	Individual			As required	until staff age 100	Employment law	
	Emergency contact	Name	Third party	Vital interests	Appointment of staff	Regularly	Until staff leaves	No business requirement	
		Contact details							
DIRECT MARKETING	Existing customers	Name	Individual	Consent of individual	First contact	?	End of relationship (unless they still want to hear from us) or consent withdrawn	Data Protection Act	Third party marketing provider held on cloud server in US
		Address				?			
		Email				?			
		Mobile				?			
		Phone				?			
	Former Customers	Name	Individual	Consent of individual	First contact	?	Relationship ended - consent still valid? **Find out more**	Data Protection Act	
		Address				?			
		Email				?			
		Mobile				?			
		Phone				?			
	Potential customers	Name	Third party list/internet	**Not sure - Find Out**	?	?	**? Not sure - find out**		**? Not sure - find out**
		Email				?			

Page 17 of 17

Isle of Man Information Commissioner – GDPR Toolkit Part 1, V1.1, May 2016

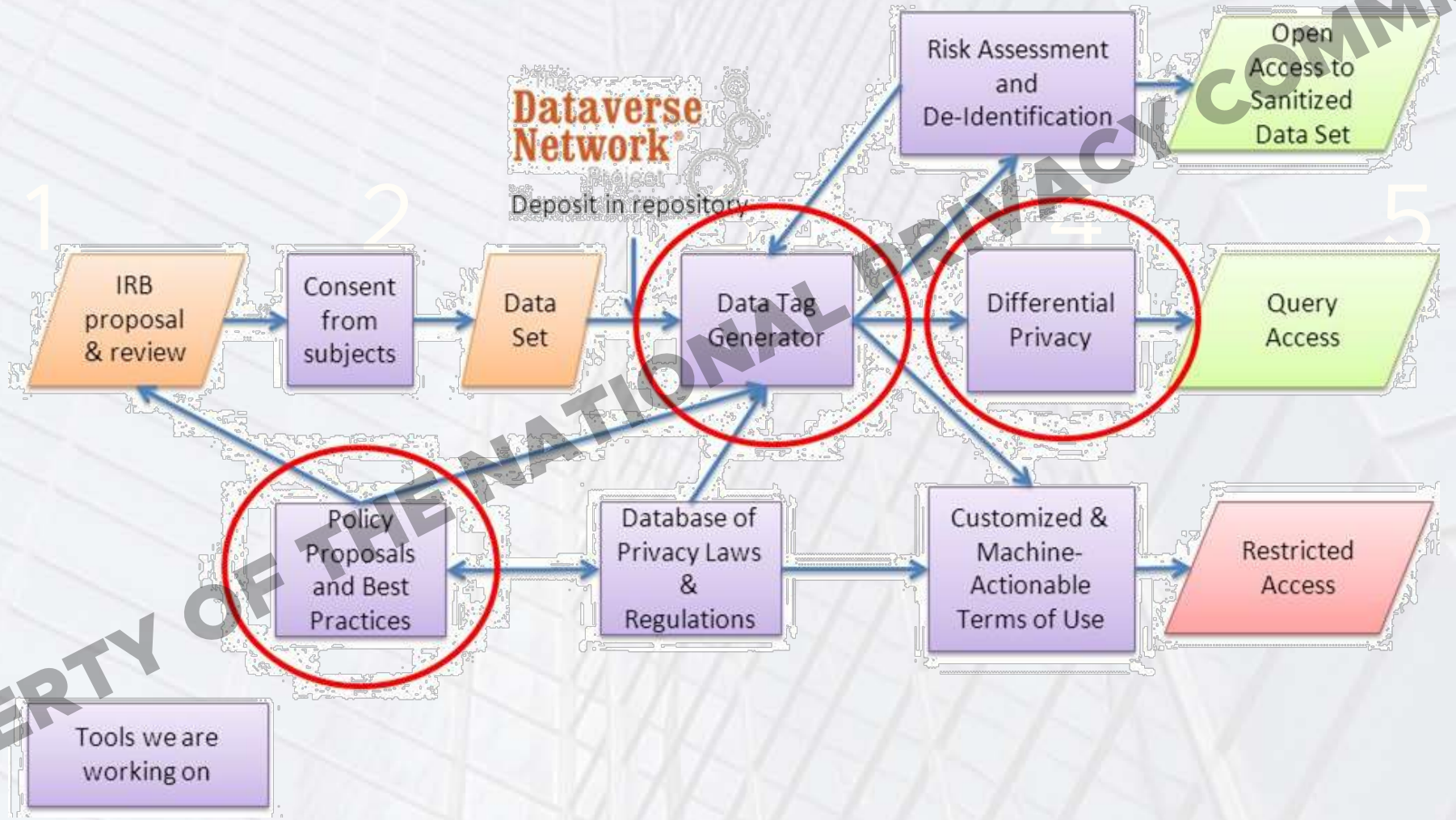
Source: http://blog.thomasbrand.xyz/wp-content/uploads/2017/08/datainventory-744x519.png

Risk Assessment

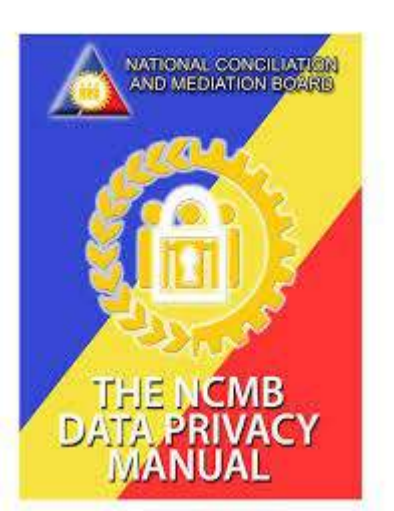
- Risk assessments should be conducted for all new projects involving personal data and on any new collection, use or disclosure of personal data.

- PICs and PIPs should develop a process for identifying and mitigating leakage and security risks which could include the use of privacy impact assessments (PIAs).

Vision: Integrated Privacy Tools



Policies and Procedures



Source: ncmb.gov.ph

- PICs and PIPs should develop and document internal policies that address obligations under the law and which should be make available to all employees and periodically updated.

- PRIVACY MANUAL - PICs and PIPs should develop internal policies that give effect to the data protection principles in the law. The internal policies should be documented and should show how they connect to the legal requirements. These policies include the following:
  - COLLECTION of personal data
  - ACCURACY and RETENTION of personal data
  - USE of personal data including the requirements for consent
  - SECURITY of personal data
  - TRANSPARENCY of their personal data policies and practices; and
  - ACCESS to and CORRECTION of personal data

Security Measures

- The PIC or PIP should have in place organizational, physical and technical security measures for purpose of maintaining the confidentiality, integrity and availability of personal data. These measures should include:

1. Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;

2. A security policy with respect to the processing of personal information

3. A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

4. Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

Capacity Building

- Orientation or training programs regarding privacy or security policies should be provided to employees.

1 2 3 4 5

- Additional training specifically tailored to their roles should be given to those who handle personal data. The training and education should be current and relevant.

Registration and Notification Requirements

The PMP should ensure compliance with the notification and reporting requirements under the Data Privacy Act. These include:

a. Registration of personal data processing systems operating in the country when the PIC or PIP employs at least 250 employees, when processing involves sensitive personal information of at least one thousand (1,000) individuals, when processing is not occasional, or when processing poses a risk to the rights and freedoms of data subjects.

b. Notification of automated processing operations where the processing becomes the sole basis of making decisions that would significantly affect the data subject;

c. Breach notification and annual report of the summary of documented security incidents and personal data breaches;

Breach Management

- PICs and PIPs should have a procedure in place and an officer or a designated team responsible for managing a personal data breach.

- Responsibilities for internal and external reporting of the breach should be clear.

- In handling personal data breach, PICs and PIPs should consider the circumstances of the breach and decide whether any of the persons identified in NPC Circular No. 16-03 should be notified.

PIP Management

- The types of obligations to be imposed on PIP should include the following:
  - SECURITY MEASURES to be taken
  - Timely RETURN, DESTRUCTION or DELETION of the personal data no longer required
  - Prohibition against other USE and DISCLOSURE
  - Prohibition (absolute or qualified) against SUB-CONTRACTING to other service provider
  - REPORTING of irregularity
  - MEASURES to ensure contract staff's compliance with the agreed obligations
  - PICs right to AUDIT and INSPECT
  - CONSEQUENCES for violation of the contract

For additional guidelines you may refer to "Rule X. Outsourcing and Sub-contracting Agreements" of the Implementing Rules and Regulations (IRR)

Communication

- Communication should be clear and easily understandable and not simply a reiteration of the Data Privacy Act. In general it should:

  - Provide enough information so that the public knows the purpose of the collection, use and disclosure of personal data and how long it is retained;
  - Include information on who to contact with questions or concerns; and
  - Be made easily available to individuals

CONTINUING ASSESSMENT and REVISION

OVERSIGHT and REVIEW PLAN

- **Develop Oversight and Review Plan**
  - This will help PICs and PIPs keep its PMP on track and up-to-date.
  - The DPO should develop an Oversight and Review Plan on a periodic basis that sets out how and when the PMP's effectiveness will be monitored and assessed.
  - The oversight and review plan should establish performance measures and include a schedule of when the policies and other program controls will be reviewed.

ASSESS and REVISE PROGRAM CONTROLS

- **Updates and Revision**
  - The effectiveness of program controls should be **monitored regularly**, **audited periodically** and where necessary, **revised accordingly**.

  - The monitoring should address the following questions:
    - What are the latest threats and risks?
    - Are the program controls addressing new threats and reflecting the latest complaint or audit findings?
    - Are new services being offered involve increased collection, use or disclosure of personal data?
    - Is training necessary? If yes, is it taking place? Is it effective? Are policies and procedures being followed? Is the training up-to-date?

ASSESS and REVISE PROGRAM CONTROLS

- **Review and Monitoring**
  - Schedule Regular PIA
  - Review Forms, Contracts, Policies, and Procedures on a regular basis
  - Review, Validate and Revise Privacy Manual.

Data Privacy Accountability and Compliance Framework

THE DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK

I. GOVERNANCE

A. Choose a DPO

II. RISK ASSESSMENT

B. Register
C. Records of processing activities
D. C[illegible]t PIA

III. ORGANIZATION

E. Privacy Management Program
F. Privacy Manual

IV. DAY TO DAY

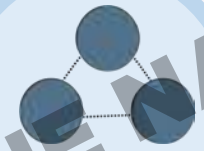
G. Privacy Notice
H-O. Data Subject Rights
P. Data Life Cycle

V. DATA SECURITY

Q. Organizational
R. Physical
S. Technical
- Data Center
- Encryption
- Access Control Policy

VI. BREACHES

T. Data Breach Management;
- Security Policy
- Data Breach Response Team
- Incident Response Procedure
- Document
- Breach Notification



VII. THIRD PARTIES

U. Third Parties;
- Legal Basis for Disclosure
- Data Sharing Agreements
- Cross Border Transfer Agreement

VIII. MANAGE HR

V. Trainings and Certifications
W. Security Clearance

IX. CONTINUITY

X. Continuing Assessment and Development
- Regular PIA
- Review Contracts
- Internal Assessments
- Review PMP
- Accreditations

X. PRIVACY ECOSYSTEM

Y. New technologies and standards
Z. New legal requirements

NATIONAL PRIVACY COMMISSION

Government DPO Conference 2018

GOVERNMENT DPO CONFERENCE 2018

Contact us

PrivacyPH

privacy.gov.ph

www.privacy.gov.ph

09451534299
09399638715

or

Email us at
info@privacy.gov.ph
compliancesupport@privacy.gov.ph
complaints@privacy.gov.ph

Address:

5th Floor, Delegation Building,
Philippine International Convention
Center (PICC) Complex, Roxas
Boulevard, Manila

Thank you!

NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 2018