



DATA PRIVACY ACT: Its Impact to the Organization

PAGBA: Building High Trust Society Thru
Strong PFM Leading to Shared Growth
July 26, 2017



What the **law** is all about



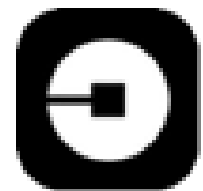
How it will affect **you**

The world's
largest taxi
company,
owns **no**
vehicles.

The world's
most popular
media owner,
creates **no**
content.

The world's
most valuable
retailer, has
no inventory.

The world's
largest
accommodation
provider, owns
no real estate.



UBER



FACEBOOK

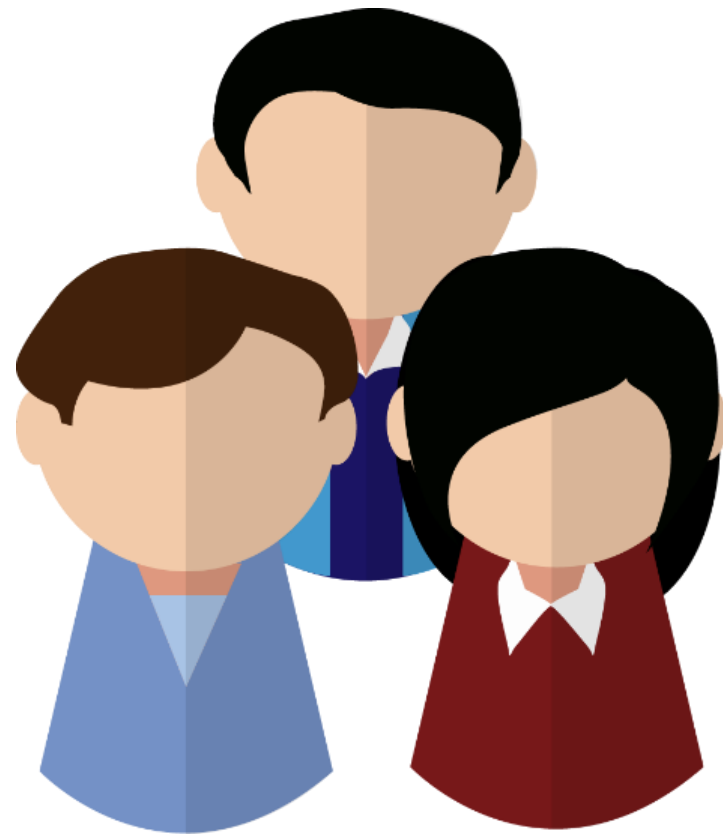


ALIBABA



AIRBNB

PROCESSING PERSONAL INFORMATION CAN CREATE PROBLEMS FOR INDIVIDUALS



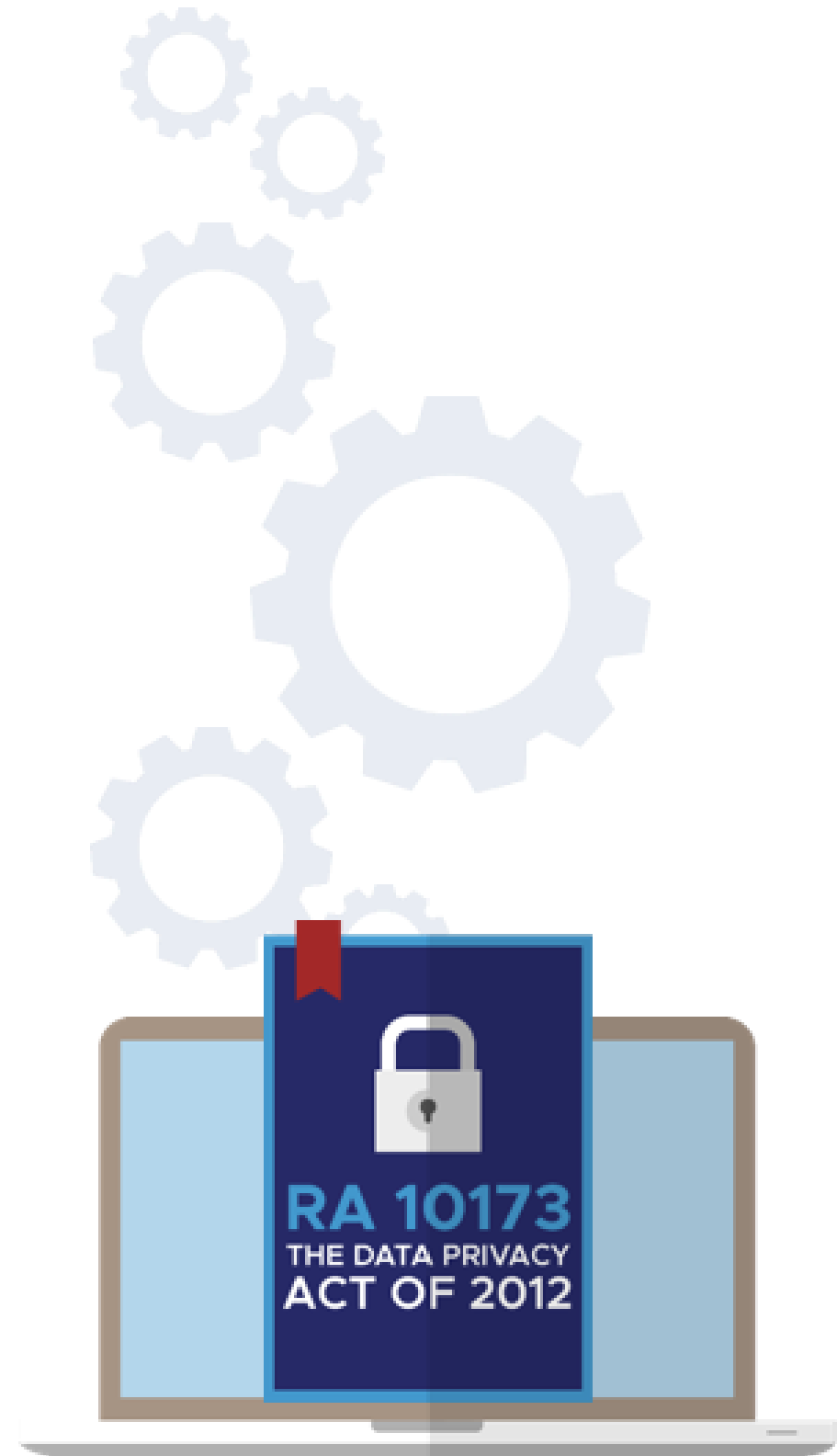
- Loss of trust
- Loss of self-determination
 - *Loss of autonomy*
 - *Loss of liberty*
 - *Exclusion*
 - *Physical harm*
- Discrimination
 - *Stigmatization*
 - *Power imbalance*
- Economic loss



INTRODUCTION: RA 10173



An act protecting individual personal information in information and communications systems in the government and the private sector, creating for this purpose a National Privacy Commission, and for other purposes.



WHERE IS *PRIVACY* IN ALL
THIS?



*The law upholds the right to privacy by **protecting** individual personal information.*

*The National Privacy Commission protects individual personal information by **regulating** the processing of personal information.*



STRUCTURE OF RA 10173

Sections 1-6.
Definitions and
General Provisions
.....

Sections 7-10.
The National
Privacy
Commission
.....



Sections 25-37.
Penalties
.....

Sections 22-24.
Provisions
Specific
to Government
.....

Sections 11-21.
Rights of Data Subjects, and Obligations of
Personal Information Controllers and Processors
.....



SEC. 2. Protect the **fundamental human right of privacy** of communication while ensuring free flow of information to promote innovation and growth; role of information and communications technology to ensure that personal information under the custody of the government and private sector are secured.

SCOPE



- ✂ **SEC. 4.** Applies to the **processing of all types of personal information**, in the country and even abroad, subject to certain qualifications.
- ✂ **SEC. 15.** Personal information controllers may invoke the **principle of privileged communication** over privileged information that they lawfully control or process.

CREATION OF THE COMMISSION



The *National Privacy Commission* protects individual personal information and upholds the **right to informational privacy** by regulating the processing of personal information.





KEY CONCEPTS



CLASSIFICATION OF PERSONAL DATA



Personal Information:

Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Sensitive Personal Information.

Refers to personal information about an individual's:

race, ethnic origin, marital status, age, color, religious, philosophical or political affiliations, health, education, genetics, sexual life, any proceeding for any offense committed or alleged to have been committed, the disposal of such proceedings, the sentence of any court in such proceedings;

Also includes information issued by government agencies peculiar to an individual which includes, but not limited to:

social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns;

and specifically established by an executive order or an act of Congress to be kept classified.



Personal Information	Sensitive Personal Information (List based on IRR)	Privileged Information (List based on Rules of Court)
Name	Race	Data received within the context of a protected relationship – husband and wife
Address	Ethnic origin	
Place of work	Marital status	
Telephone number	Age	
Gender	Color	Data received within the context of a protected relationship – attorney and client
Location of an individual at a particular time	Religious affiliation	
IP address	Philosophical affiliation	
Birth date	Political affiliation	
Birth place	Health	Data received within the context of a protected relationship – priest and penitent
Country of citizenship	Education	
Citizenship status	Genetics	
Payroll & benefits information	Sexual life	
Contact information	Proceeding for any offense committed or alleged to have been committed, the disposal of such proceedings, the sentence of any court in such proceedings	Data received within the context of a protected relationship – doctor and patient

	Sensitive Personal Information (List based on IRR)	
	<i>Social security number</i>	
	<i>Licenses or its denials, suspension or revocation</i>	
	<i>Tax returns</i>	
	<i>Other personal info issued by government agencies</i>	
	<i>Bank and credit/debit card numbers</i>	
	<i>Websites visited</i>	
	<i>Materials downloaded</i>	
	<i>Any other information reflecting preferences and behaviors of an individual</i>	
	<i>Grievance information</i>	
	<i>Discipline information</i>	
	<i>Leave of absence reason</i>	
	<i>Licenses or its denials, suspension or revocation</i>	

PROCESSING



Any operation of any set of **operations performed upon personal data** including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

PERSONAL INFORMATION CONTROLLER



Refers to a natural or juridical person, or any other body who **controls the processing of personal data**, or instructs another to process personal data on its behalf.

It excludes:

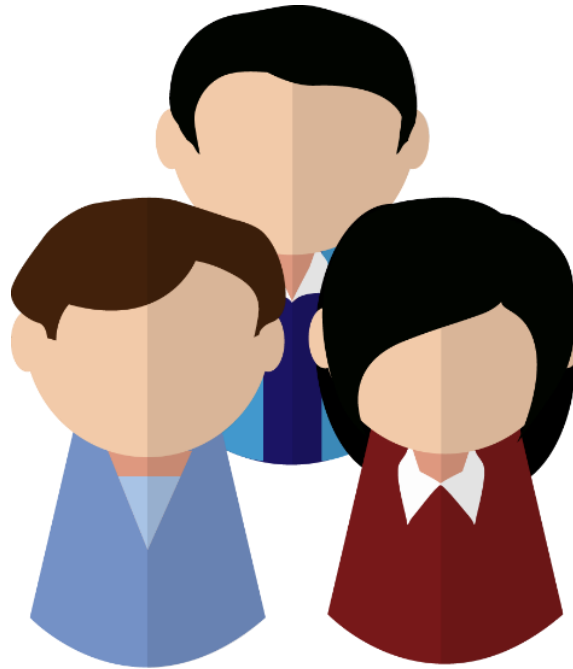
- ✂ A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
- ✂ A natural person who processes personal data in connection with his or her personal, family, or household affairs;

PERSONAL INFORMATION PROCESSOR

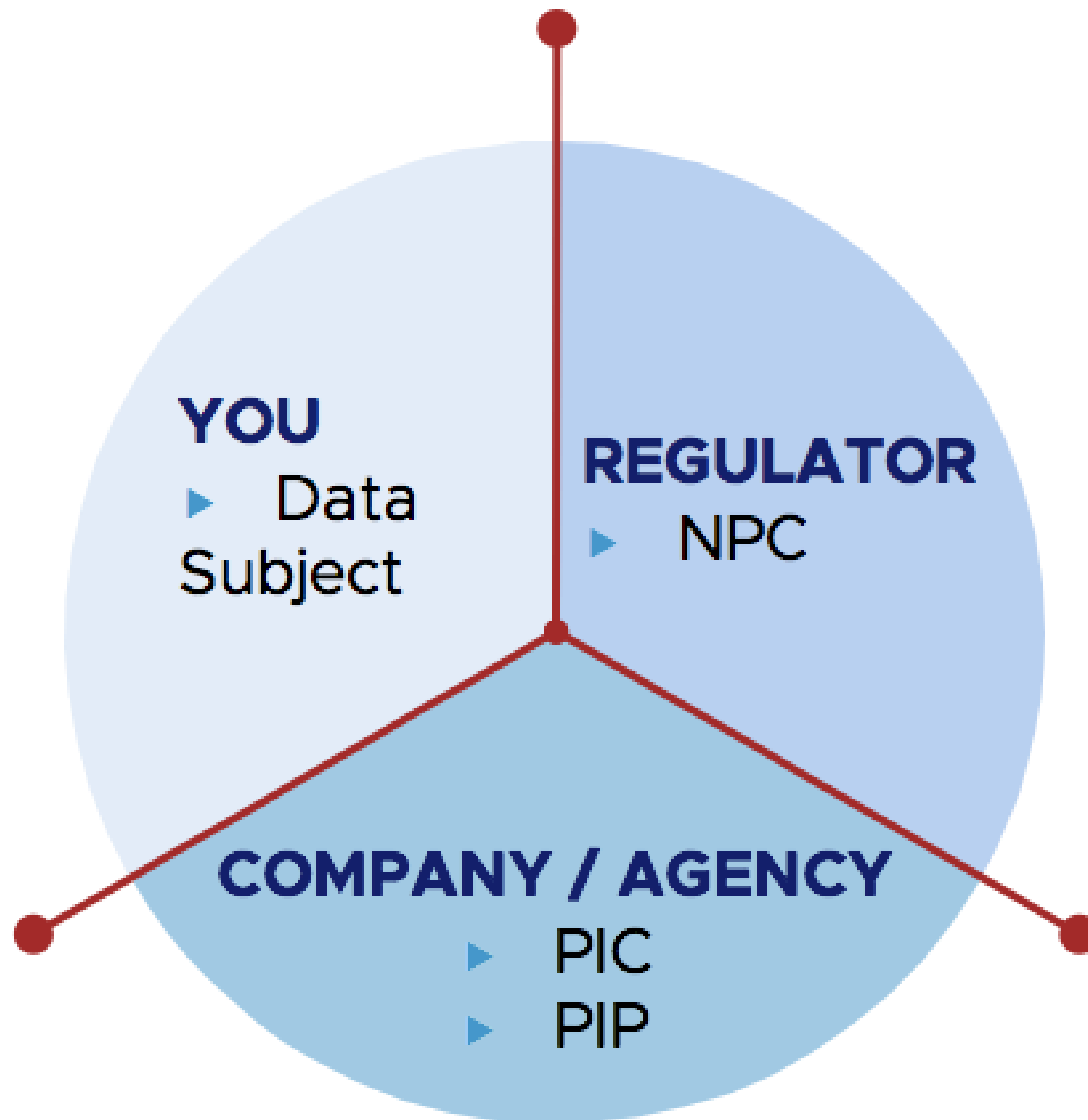


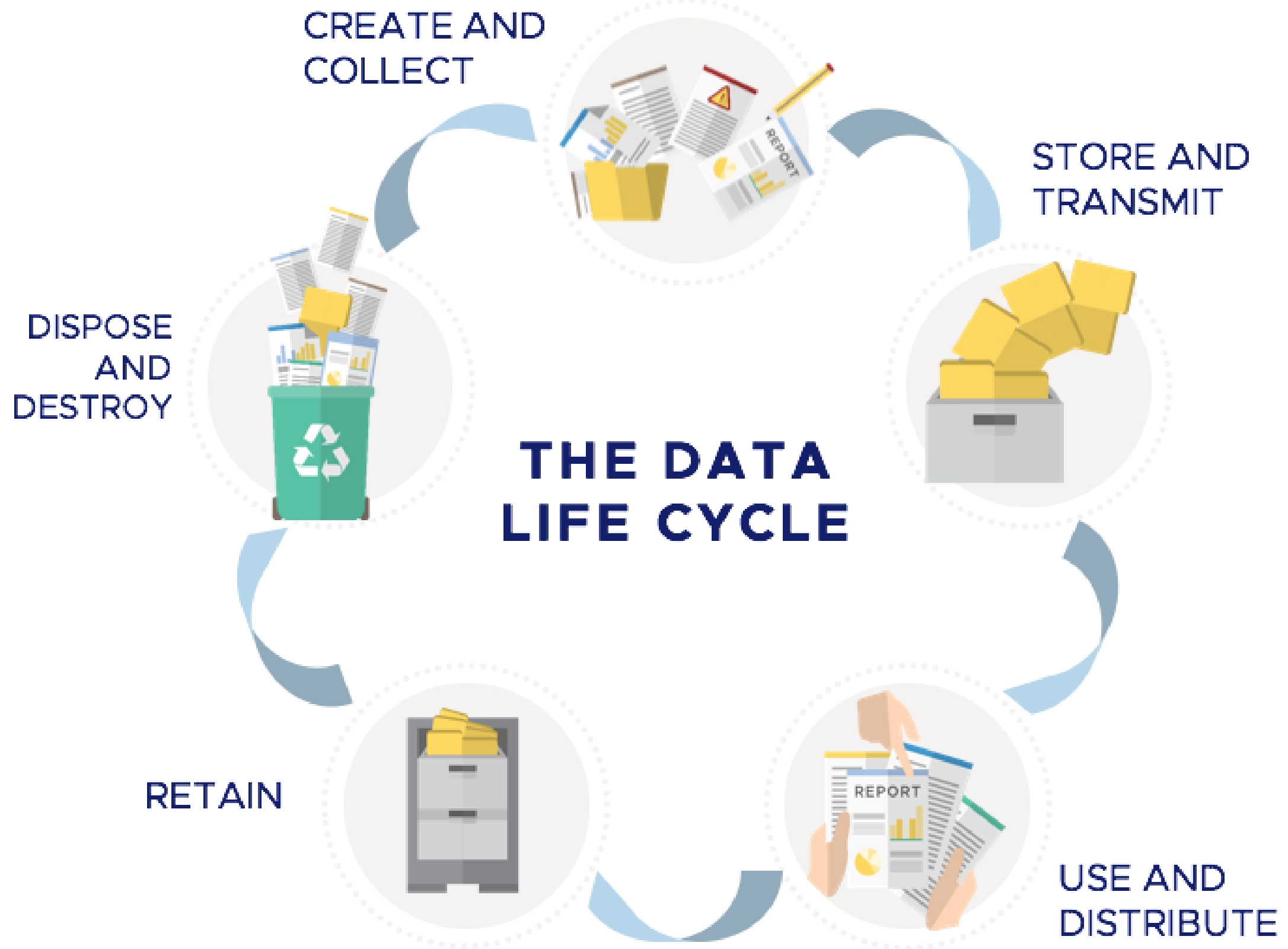
Refers to any natural or juridical person or any other body to whom a personal information controller may **outsource or instruct the processing of personal data** pertaining to a data subject.

DATA SUBJECT



An individual whose **personal, sensitive personal or privileged information is processed.**



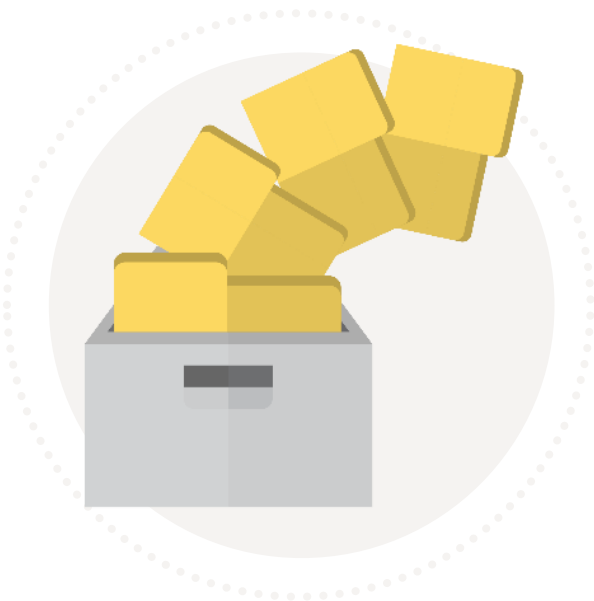


I. CREATE AND COLLECT



Punishable Act	Imprisonment	Fine (PHP)
Unauthorized Purposes	18 months to 5 years — 2 years to 7 years	500 thousand to 2 million
Unauthorized Processing of Personal Information/Records	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million

II. STORE AND TRANSMIT



Punishable Act	Imprisonment	Fine (PHP)
Accessing of Personal Information and Sensitive Personal Information due to Negligence	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Intentional Breach	1 year to 3 years	500 thousand to 2 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 2 million

III. USE AND DISTRIBUTE



Punishable Act	Imprisonment	Fine (PHP)
Unauthorized Processing of Personal Information and Sensitive Personal Information	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Unauthorized Purposes	18 months to 5 years — 2 years to 7 years	500 thousand to 2 million
Intentional Breach	1 year to 3 years	500 thousand to 2 million
Concealing Breach	18 months to 5 years	500 thousand to 1 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 2 million

IV. RETAIN



Punishable Act	Imprisonment	Fine (PHP)
Access due to Negligence of Records	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 1 million

V. DISPOSE AND DESTROY



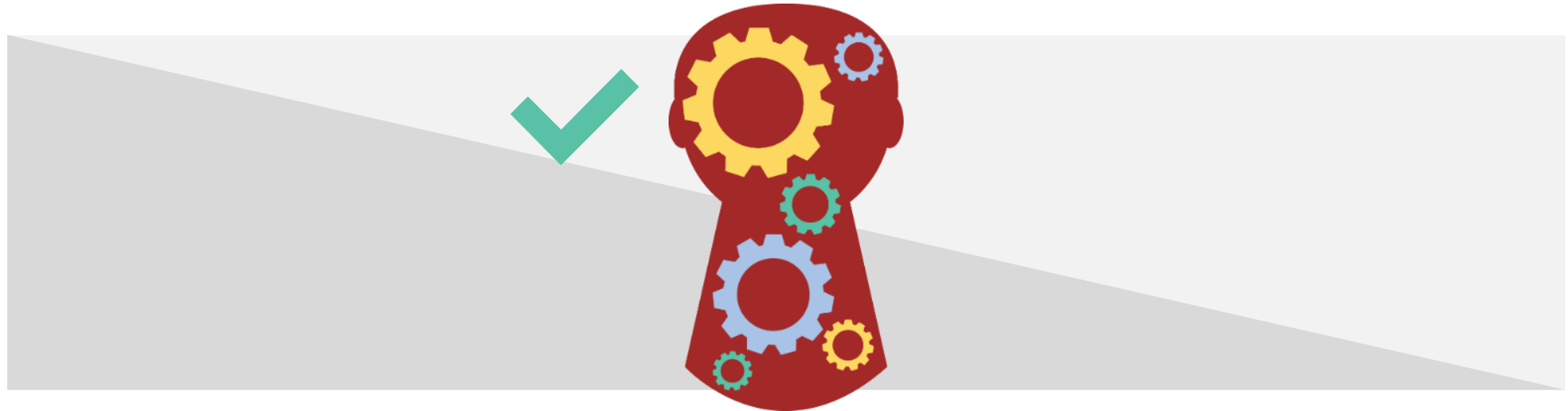
Punishable Act	Imprisonment	Fine (PHP)
Improper Disposal of Records	6 months 2 years — 1 year to 3 years	100 thousand to 1 million
Access due to Negligence	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Concealing Breach	18 months to 5 years	500 thousand to 1 million

SPECIAL CASES

The law shall not apply to the following **specified information**:

- a. Information of public concern;
- b. Personal information for journalistic, artistic, or literary purpose, subject to requirements of other applicable laws or regulations;
- c. Personal information for research purposes, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards;
- d. Information necessary in order to carry out the functions of public authority;
- e. Information necessary for banks, other financial institutions, to the extent necessary to comply with applicable laws; and
- f. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions.

TRANSPARENCY



Principle of Transparency

A data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

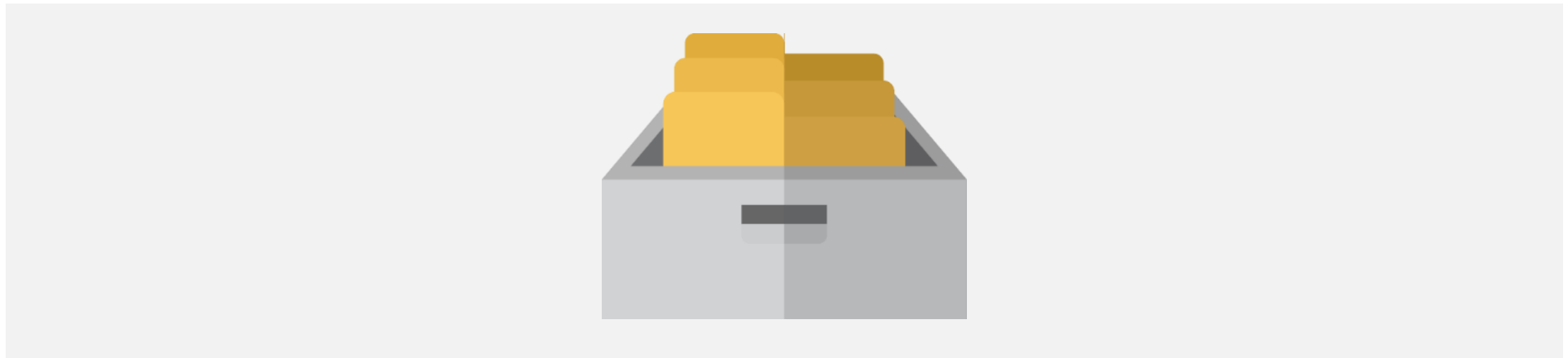
LEGITIMATE PURPOSE



Principle of Legitimate Purpose


The processing of information shall be compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy.

PROPORTIONALITY



Principle of Proportionality

The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.



THE FIVE PILLARS OF COMPLIANCE



Commit to
Comply: Appoint a
**Data Protection
Officer (DPO)**



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



Be Accountable:
Create your
**Privacy
Management
Program and
Privacy Manual**



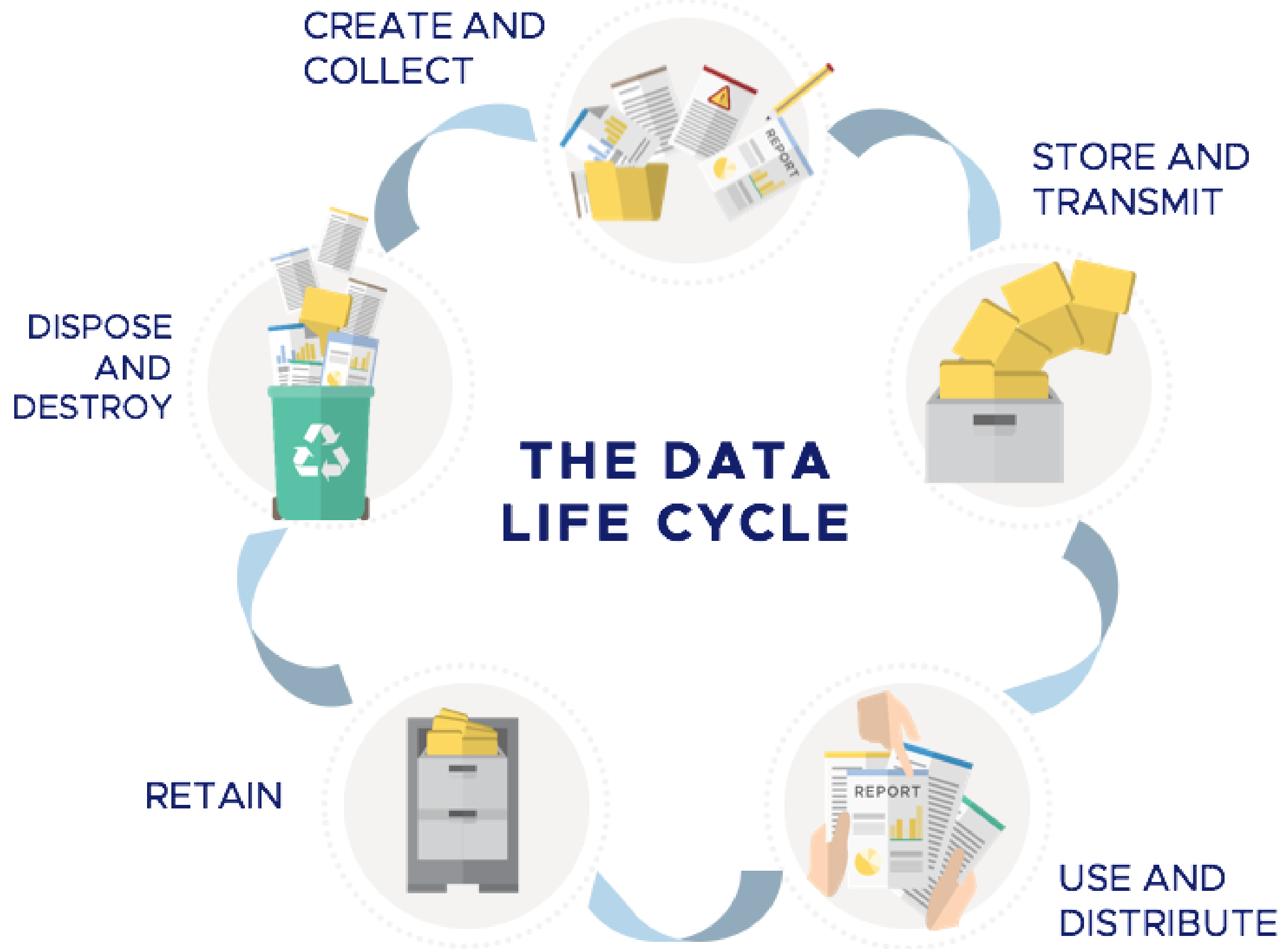
Demonstrate Your
Compliance:
Implement your
**privacy and data
protection (PDP)**
measures.



Be Prepared for
Breach:
Regularly exercise
your **Breach
Reporting
Procedures (BRP)**.

THE DATA PRIVACY COMPLIANCE AND ACCOUNTABILITY FRAMEWORK





I. GOVERNANCE



Choose a DPO
Register

I. GOVERNANCE

Framework

Appointment of your Data Privacy Officer (DPO)

Register Data Processing Systems (Phase I)

Demonstrate Compliance (Output/Evidence)

Designation / Appointment Papers / Contract of the DPO and / or DPO team

Website or other visible announcement showing contact details of DPO

NPC Notification of completing Phase I Registration

Other means to demonstrate compliance

II. RISK ASSESSMENT



Conduct PIA

II. RISK ASSESSMENT

Framework

Maintain records of processing activities, including inventory of personal data, data flow and transfers outside country

Conduct a Privacy Impact Assessment (PIA) including baselining (Personal Data Inventory)

Demonstrate Compliance (Output/Evidence)

Records of Processing Activities

PIA Report

Other means to demonstrate compliance

III. ORGANIZATION



Privacy Management Program
Privacy Manual

III. ORGANIZATION

Framework

Implement and Maintain a Privacy Management Program (PMP)

Develop a Privacy Manual

Demonstrate Compliance (Output/Evidence)

Privacy Manual

List of activities on privacy and data protection

List of key personnel assigned responsibilities for privacy and data protection within the organization

Other means to demonstrate compliance

IV. DAY TO DAY OPERATIONS



Privacy Notice
Data Subject Rights
Retention
Disposal

IV. DAY TO DAY OPERATIONS

Framework

Have visible and accessible Privacy Notices with contact details of DPO

Develop, Review or Maintain Policies and Procedures for processing of personal data from collection to retention or disposal (procedure for obtaining consent)

Establish procedures or platform for data subjects to exercise their rights (access, correction erasure, data portability)

Register Data Processing Systems (Phase II)

Comply with notification and reporting requirements

Demonstrate Compliance (Output/Evidence)

Privacy Notice in Website and / or within organization (where collection of personal data occurs)

Consent forms for collection and use of personal data

List of Policies and Procedures in place that relate to privacy and data protection (may be in privacy manual)

Policies and Procedures in dealing with requests for information from parties other than the data subjects (media, law enforcement, representatives)

Retention and Disposal Schedules

IV. DAY TO DAY OPERATIONS

Demonstrate Compliance (Output/Evidence)

Policies and Procedures in dealing with requests for information from parties other than the data subjects (media, law enforcement, representatives)

Retention and Disposal Schedules

Policies and Procedure for data subjects to exercise rights (may be in Privacy Manual)

Data subjects informed of rights through privacy notices, and other means

Form or platform for data subjects to request copy of their personal information and request correction

Procedure for addressing complaints of data subjects

Certificate of registration and notification

Other means to demonstrate compliance

IV. DAY TO DAY OPERATIONS

Informing data subjects of your personal information processing activities and obtain their consent, when necessary. (Privacy Notice)

Formulation of policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them

CREATION AND COLLECTION

Policies for limiting data processing according to its declared, specified and legitimate purpose?

Policies/procedures for providing data subjects with access to their personal information including its sources, recipients, method of collection, purpose of disclosure to third parties, automated processes, date of last access, and identity of the controller (Data Subject Access Request)

Policies/procedures that allow data subjects to dispute inaccuracy or error of their personal information including policies/procedures the same up to date

Policies/procedures that allow a data subject to suspend, withdraw or order the blocking, removal or destruction of their personal information

STORAGE, TRANSMISSION, USE AND DISTRIBUTION

Policies/procedures for accepting and addressing complaints from data subjects

Policies/procedures for retaining personal data for only a limited period or until the purpose of the processing has been achieved

RETENTION

Policies/procedures for ensuring that data is securely destroyed or disposed of

DESTRUCTION/DISPOSAL

V. DATA SECURITY



Data Center
Encryption
Access Policy
Transfers

V. DATA SECURITY

Framework

Maintain Organizational Security Measures (Policies and procedures in place)

Maintain Physical Security Measures (Physical Access and Security, Design and Infrastructure)

Maintain Technical Security Measures (Firewalls, Encryption, Access Policy, Security of Transfers and Storage of Data, other Information security tools)

Demonstrate Compliance (Output/Evidence)

Data Center and Storage area with limited physical access

Report on technical security measures and information security tools in place

Firewalls used

Encryption used for transmission

Encryption used for storage

Access Policy for onsite, remote, and online access

Audit logs

Back-up solutions

Report of Internal Security Audit or other internal assessments

Certifications or accreditations maintained

Other means to demonstrate compliance

V. DATA SECURITY

Compliance with the DPA's Data Storage Requirements

Encryption

Compliance with the DPA's control access requirements for personal data
(onsite, remotely, or online)

Compliance with the DPA's requirements for Personal Data Transfers



VI. BREACHES



Breach Management

Assessment
Monitoring
Response Team
Review
Notification

VI. BREACHES

Framework

Implement safeguards to prevent or minimize personal data breach (Breach drills, security policy)

Constitute Data Breach Response Team

Maintain and Review Incident Response Policy and Procedure

Document Security Incidents and personal data breaches

Comply with Breach Notification requirements

Demonstrate Compliance (Output/Evidence)

Schedule of breach drills

Number of Trainings conducted for internal personnel on breach management

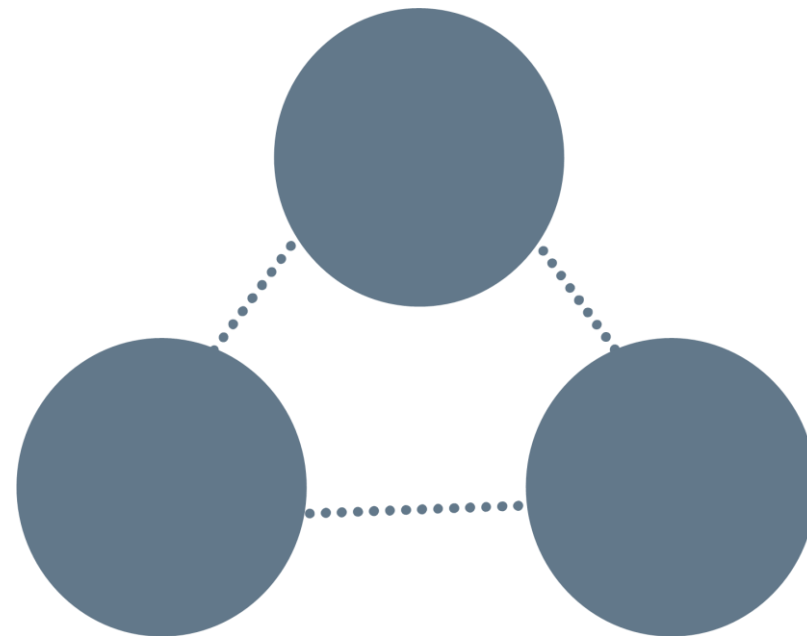
Personnel Order constituting the Data Breach Response Team

Incident Response Policy and Procedure (may be in Privacy Manual)

Record of Security incidents and personal data breaches, including notification for personal data breaches

Other means to demonstrate compliance

VII. THIRD PARTIES



Due Diligence
Agreements
Notification
Access Policy

VII. THIRD PARTIES

Framework

Execute Data Sharing Agreements

Review or Enter into contracts and other agreements for transfers of personal data, including cross border transfers, to ensure comparable level of data protection and DPA compliance

Review or enter into outsourcing contracts with PIPs, to ensure comparable level of data protection and DPA compliance

Establish and document legal basis for disclosures of personal data made to third parties

Demonstrate Compliance (Output/Evidence)

Data Sharing Agreements

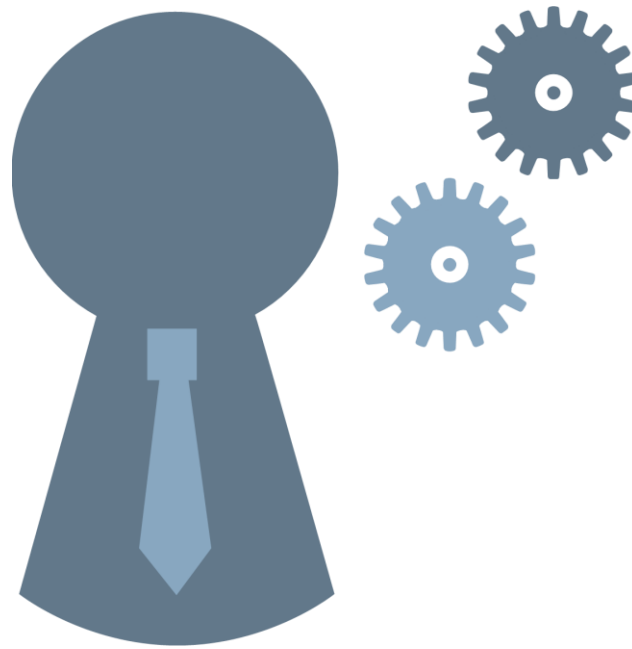
List of recipients of personal data (PIPs, other PICs, service providers, government agencies)

Review of Contracts with PIPs

Review of Contracts for cross-border transfers

Other means to demonstrate compliance

VIII. MANAGE HR



Training

VIII. MANAGE HR

Framework

Regularly train personnel regarding privacy or security policies

Ongoing training and capacity building for Data Protection Officer

DPOs work towards certifications and applies for membership in DPO organizations

Non-Disclosure Agreements for personnel handling Data

Security Clearance issued for those handling personal data

Demonstrate Compliance (Output/Evidence)

Number of employees who attended trainings on privacy and data protection

Commitment to comply with Data Privacy Act as part of Code of Conduct or through written document to be part of employee files

Certificate of Training of DPO

Certifications of DPOs

NDA's or confidentiality agreements

Other means to demonstrate compliance

IX. PROJECTS



Conduct and Update PIA

IX. PROJECTS

Framework

Schedule Regular PIA

Review Forms, Contracts, Policies and Procedures on a regular basis

Schedule Regular Compliance monitoring, internal assessments, and security audits

Review, Validate and Revise Privacy Manual

Regularly evaluate Privacy Management Program

Demonstrate Compliance (Output/Evidence)

Policy for Conduct of PIA (may be in manual)

Policy on conduct of Internal Assessments and Security Audits

Privacy Manual contains policy for regular review

List of activities to evaluate Privacy Management Program (survey of customer, personnel assessment)

Other means to demonstrate compliance

X. MANAGE LEGAL COMPLIANCE



Monitor Legal Compliance
Contract Review

X. MANAGE LEGAL COMPLIANCE

Framework

Monitor emerging technologies, new risks of data processing, and the legal and ICT Environment

Keep track of data privacy best practices, sector specific standards, and international data protection standards

Attend trainings and conferences

Seek guidance and legal opinion on new NPC Issuances or requirements

Demonstrate Compliance (Output/Evidence)

Number of trainings and conferences attended on privacy and data protection


Policy papers, legal or position papers, or other research initiatives on emerging technologies, data privacy best practices, sector specific standards, and international data protection standards

Number of management meetings which included privacy and data protection in the agenda


Other means to demonstrate compliance

I. Establishing Data Privacy Governance	
1. Appointment of your Data Privacy Officer (DPO)	
2. Register	
II. Risk Assessment	
3. Conduct of a Privacy Impact Assessment (PIA) including baselining (Personal Data Inventory)	
III. Preparing Your Organization's Data Privacy Rules	
4. Formulate your organization's privacy management program (PMP)	
5. Craft your agency's privacy manual	
IV. Privacy in Day-to-Day Information Life Cycle Operations (To Be Included in the Privacy Manual)	
6. Informing data subjects of your personal information processing activities and obtain their consent, when necessary. (Privacy Notice)	CREATION AND COLLECTION
7. Formulation of policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them	
8. Policies for limiting data processing according to its declared, specified and legitimate purpose?	STORAGE, TRANSMISSION, USE AND DISTRIBUTION
9. Policies/procedures for providing data subjects with access to their personal information including its sources, recipients, method of collection, purpose of disclosure to third parties, automated processes, date of last access, and identity of the controller (Data Subject Access Request)	
10. Policies/procedures that allow data subjects to dispute inaccuracy or error of their personal information including policies/procedures to keep the same up to date	
11. Policies/procedures that allow a data subject to suspend withdraw or order the blocking, removal or destruction of their personal information	
12. Policies/procedures for accepting and addressing complaints from data subjects.	
13. Policies/procedures for retaining personal data for only a limited period or until the purpose of the processing has been achieved.	RETENTION
14. Policies/procedures for ensuring that data is securely destroyed or disposed of	DESTRUCTION/ DISPOSAL
V. Managing Personal Data Security Risks	
15. Compliance with the DPA's Data Storage Requirements	
16. Encryption	
17. Compliance with the DPA's control access requirements for personal data (onsite, remotely or online)	
18. Compliance with the DPA's requirements for Personal Data Transfers	
VI. Data Breach Management	
19. Compliance with the DPA's Data Breach Management Requirements.	
VII. Managing Third Party Risks	
20. Maintaining data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)? (Compliance, Agreements, Due Diligence, Notifications, Access Policies)	
VIII. Managing Human Resources (HR)	
21. Periodic and mandatory personnel training on privacy and data protection in general and in areas reflecting job-specific content.	
IX. Monitoring Mechanisms for New and Current Projects	
22. Conducting or updating Privacy Impact Assessments for new and existing programs, systems, processes and projects	
X. Managing Your Legal Environment	
23. Policies/procedures for monitoring and complying with the applicable legal requirements.	

UPDATES ON THE ONGOING IMPLEMENTATION OF THE DPA



*The **National Privacy Commission** has been invited to numerous events and meetings hosted by both the government and the privacy sector to provide an orientation on the DPA, IRR and issuances of the Commission.*



MEASURES FOR UPHOLDING THE RIGHT TO PRIVACY AND DATA SECURITY



- ♦ Bank and other financial institutions should **designate or appoint their Data Protection Officers**. Such professionals who process personal data are themselves de facto Compliance Officers for Privacy. They should perform their duties and responsibilities, as such.
- ♦ Bank and other financial institutions should **conduct a privacy impact assessment (PIA)** vis-à-vis their data processing systems.
- ♦ Bank and other financial institutions should **develop and maintain a privacy manual**, which outlines how their personnel will comply with data privacy policies and uphold the rights of data subjects.

NATIONAL
PRIVACY
COMMISSION

PDS Group

Philippine Dealing & Exchange Corp. (PDEX)
Depository & Trust Corp. (PDTC)
Securities Settlement Corp. (PSSC)



Talk with corporate leaders and representatives from the Capital Market Industry at the Philippines Dealings System Holdings Corp.





*Bankers Association of
the Philippines*





*54th Annual Convention of the
Philippine Pediatric Society*





*How to Comply: Jumpstarting Your Compliance
with the R.A. 10173 roadshow in Zamboanga
City.*





*First Data Protection Officers'
Assembly (DPO1) for the
Government*






*Second Data Protection
Officers' Assembly (DPO1) for
the Banking Sector*



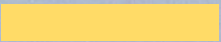
29

The **Commission** continues to accept requests for opinions/clarifications on the interpretation of the provisions of the DPA and IRR, and have released twenty-nine (29) advisory opinions as of today.





The **Commission** likewise
provide comments and
position papers on bills with
the Senate and House of
Representatives which has
privacy implications





NATIONAL
PRIVACY
COMMISSION

PRIVACY.GOV.PH

facebook.com/privacy.gov.ph

twitter.com/privacyph

info@privacy.gov.ph