The Data Privacy Act (2012)

Atty. Rejyl B. Siang
Compliance and Monitoring Division
National Privacy Commission
What is Privacy in Filipino?

If I post a picture on Facebook, is it’s use free-for-all?

If I open a savings account, can the bank use my personal information to open a credit card account?

If I subscribe to a mobile plan, can the telco sell my information to telemarketers or loan agencies?
What is private then – what is found within the four corners of your home and within the confidentiality of communication.

SECTION 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable...

SECTION 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.

Art. 26. Every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons. (Prying, meddling, intriguing, vexing or humiliating)

Art III, 1987 Constitution

Art III, 1987 Constitution

New Civil Code
What is private now –

what he seeks to preserve as private, even in a public area...
DATA PRIVACY IS ABOUT

1. **PEOPLE**, NOT PLACES

2. **PERSONAL CHOICE**

3. **CONTROL**, NOT SECRECY

4. **THE RIGHT TO BE LET ALONE**
The 4th Industrial Revolution: 
*Data as the new oil of the digital economy?*

1st Industrial Revolution: Mechanization, water power, steam power
2nd Industrial Revolution: Mass production, assembly line, electricity
3rd Industrial Revolution: Computer and automation
4th Industrial Revolution: Cyber physical system

- Maturation of new cyber physical technologies (artificial intelligence, 3-D printing, robotics)
- Data analytics driving efficiency and new business models
- Pervasive sensing and actuation
- Ubiquitous connectivity throughout the supply chain
- Unprecedented levels of data and increased computing powers

Source: *Forbes*; World Economic Forum

McKinsey & Company
DATA PROTECTION
CONFIDENTIALITY
AVAILABILITY
INTEGRITY

DATA PRIVACY
ACCOUNTABILITY
ASSURANCE
OPERATIONAL COMPLIANCE
DEMONSTRABLE COMPLIANCE
Privacy Breaches: Examples

- lost or stolen laptops, removable storage devices, or paper records containing personal information
- hard disk drives and other digital storage media being disposed of or returned to equipment lessors without the contents first being erased
- databases containing personal information being ‘hacked’ into or otherwise illegally accessed by individuals outside of the agency or organization
- employees accessing or disclosing personal information outside the requirements or authorization of their employment
privacy breaches:
examples

- paper records stolen from insecure recycling or garbage bins
- an agency or organization mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address, and
- an individual deceiving an agency or organization into improperly releasing the personal information of another person.
PROCESSING PERSONAL INFORMATION CAN CREATE PROBLEMS FOR INDIVIDUALS

- Loss of trust
- Loss of self-determination
- Loss of autonomy
- Loss of liberty
- Discrimination
- Stigmatization
WHAT DOES THE LAW SAY?

■ 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.
The scope of the DPA

SEC. 4
Applies to the processing of all types of personal information, in the country and even abroad, subject to certain qualifications.
Exemptions

- Information processed for purpose of allowing public access to information that fall within matters of public concern
- Personal information processed for journalistic, artistic or literary purpose
- Personal information that will be processed for research purpose
- Information necessary in order to carry out the functions of public authority
- Information necessary for banks, other financial institutions to comply with AMLA
- Personal information originally collected from residents of foreign jurisdictions
PERSONAL INFORMATION

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.

Section 12
Conditions under which processing Personal Information is allowed...
Section 12

Conditions under which processing Personal Information is allowed... (3Cs, 2Ps, 2Is)

- Consent
- Contract
- Compliance with a legal obligation
- Respond to national emergency, public order/safety
- Fulfill functions of public authority
- Protect vitally important interests of the data subject, including life and health
- Legitimate interests
PERSONAL INFORMATION

(1) race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
(2) health, education, genetic or sexual life of a person,
(3) civil, criminal or administrative proceedings
(4) Unique identifiers issued by government agencies peculiar to an individual
(5) Specifically established by law as classified

Section 13
Processing of Sensitive Personal Information is prohibited except in the following cases...
Section 13
Processing of Sensitive Personal Information is **prohibited** except in the following cases...
(C, 2Ls, 3Ps, M)

- Consent
- Provided for by existing laws and regulations
- Protect the life and health of the data subject
- Necessary to achieve the lawful and noncommercial objectives of public organizations and their associations
- Protection of lawful rights and interests, Legal claims
- Provided to government or public authority pursuant to a constitutional or statutory mandate
- Medical treatment
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.
THE DATA LIFE CYCLE

1. CREATE AND COLLECT
2. STORE AND TRANSMIT
3. USE AND DISTRIBUTE
4. RETAIN
5. DISPOSE AND DESTROY
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 person who processes personal data in connection with his or her personal, family, or household affairs.
PERSONAL INFORMATION
PROCESSOR

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.
Obligation of PICs

General Privacy Principles
- TRANSPARENCY
- LEGITIMATE PURPOSE
- PROPORTIONALITY

Data Subject Rights
- Right to be Informed
- Right to Access
- Right to Object
- Right to Rectification
- Right to Erasure or Blocking
- Right to Damages
- Right to Data Portability
- Right to File A Complaint

Security Measures
- ORGANIZATIONAL
- PHYSICAL
- TECHNICAL
DATA PRIVACY PRINCIPLES

TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY
TRANSPARENCY

A data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data,

- Risks
- Safeguards involved
- The identity of personal information controller
- Rights as a data subject
- 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.
PAW 2019
Privacy Notice

By voluntarily signing this form, participants consent to the processing of their personal information (full name and signature) including photo and video coverage. The personal information will be used by the National Privacy Commission to document the event and contact you, if necessary. These will only be shared with concerned government agencies to comply with audit and transparency requirements mandated by applicable laws. We will retain and dispose your personal information in compliance with RA 9470, also known as the National Archives of the Philippines Act of 2007.

Under RA 10173 or the Data Privacy Act of 2012, you have the right to be informed, to object, to access, to rectification, to erasure or blocking, to damages, to data portability and to file a complaint. If you wish to exercise any of these rights, please contact our Data Protection Officer through any of the following channels:

Email: info@privacy.gov.ph
Phone: 234-22-28 ext. 116
Mailing Address: 5th Floor Delegation Building, PICC Complex, Roxas Boulevard, Pasay City
Consent

- The data subject agrees to the collection and processing
  ✓ Freely given
  ✓ Specific
  ✓ Informed indication of will

- Evidenced by written, electronic or recorded means:
  ✓ signature
  ✓ opt-in box/clicking an icon
  ✓ sending a confirmation email
  ✓ oral confirmation
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.
#DontMe

LEGITIMATE PURPOSE
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.
PARA MAKAUTANG.. (PLEASE BRING THIS REQUIREMENTS)

- 6pcs 2x2 PICTURE
- 4pcs 1x1 PICTURE (WHOLE BODY)
- 3 VALID ID'S
- BRGY. CLEARANCE
- NBI CLEARANCE
- MAYORS PERMIT
- MEDICAL
- CEDULA
- BIRTH CERTIFICATE (NSO)
- SSS/TIN
- CO-MAKER
- X-RAY (WHOLE BODY)
- POLICE CLEARANCE
- PROOF OF BILLING
- FORM 137
DATA SUBJECT RIGHTS

- The right to be informed
- The right to object
- The right to access
- The right to rectify
- The right to erasure or blocking
- The right to damages
- The right to data portability
- The right to file a complaint
Involves implementing policies and programs explicitly intended to ingrain the culture of privacy into an organization.

Refers to the practical protective schemes such as provision for security guards, padlocks, lockers and secluded archives to physically protect paper records and databases.

Covers all proactive and defensive IT solutions an organization could employ in securing its data assets against all types of breaches.
Appoint a Data Protection Officer (DPO)

- The 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.
1. Physical Security Measures
   - Physical Barriers
     - Solid walls
     - Caged-in areas
     - Bulletproof glass
     - Locked doors
     - Surveillance
     - Restricted access

2. Physical Access Controls
   - Conventional key and lock set
   - Electronic key system
   - Mechanical combination lock
   - Electronic combination lock

3. Data File Protection

4. Natural Disaster Protection
   - Heat sensors
   - Smoke Detectors
TECHNICAL SECURITY MEASURES

1. Vulnerability testing
2. Penetration testing
3. Access Control
4. Multifactor Authentication
5. Firewalls
6. Cryptography
7. Authorization
8. Antivirus
9. Encryption
10. Decryption
11. Patch Management
12. Back up Solutions
13. Threat Analysis
14. Threat Monitoring
15. Intrusion Prevention
16. Intrusion Detection
17. Web service security
18. System Logs / Audit Logs
19. Security Data Analysis
20. Security Clearance
THE FIVE 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
If you can't protect it, DON’T collect it.

The Data Privacy Golden Rule
Thank you!
Compliance Framework & Compliance Checks

Atty. Rejyl B. Siang
Compliance and Monitoring Division
National Privacy Commission
Compliance Framework & Compliance Checks
THE FIVE 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
## PMP Key Components

<table>
<thead>
<tr>
<th>Organizational Commitment</th>
<th>Program Controls</th>
<th>Continuing Assessment and Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Buy in from the Top</td>
<td>1. Records of Processing Activities</td>
<td>1. Develop an Oversight and Review Plan</td>
</tr>
<tr>
<td></td>
<td>4. Capacity Building</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Breach Handling</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Management of Personal Information Processors</td>
<td></td>
</tr>
</tbody>
</table>
**PMP Key Components**

<table>
<thead>
<tr>
<th>Organizational Commitment</th>
<th>Program Controls</th>
<th>Continuing Assessment and Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Buy in from the Top</td>
<td>1. Records of Processing Activities</td>
<td>1. Develop an Oversight and Review Plan</td>
</tr>
<tr>
<td></td>
<td>2. Policies</td>
<td>2. Assess and Revise Program Controls</td>
</tr>
<tr>
<td></td>
<td>3. Risk Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Capacity Building</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Breach Handling</td>
<td></td>
</tr>
<tr>
<td>3. Reporting Mechanisms</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EVIDENCE
Records of Processing Activities (Personal Data Inventory)

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

- Data Inventory
  - also referred to as “record of authority”
  - identifies personal data as it moves across various systems and thus how data is shared and organized, and its location. That data is then categorized by subject area, which identifies inconsistent data versions, enabling identification and mitigation of data disparities. *(Reference(s) in IAPP Certification Textbooks: M33)*
# PROGRAM CONTROLS

## RECORDS OF PROCESSING ACTIVITIES

<table>
<thead>
<tr>
<th>Name of Organization:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email:</th>
<th>Contact Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Protection Officer:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact Details:</th>
<th>Email:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Joint Controllership:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NO.</th>
<th>NAME</th>
<th>DATA SUBJECTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(Describe the categories of the data subjects.)</td>
</tr>
</tbody>
</table>

| (State the name of the data processing system.) | (State the information about the purpose of the processing of personal data, including any intended future processing or data sharing.) |
|                                               |                                                               |

|                          |                                                              |
|                          |                                                              |
## GENERAL INFORMATION

*State the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data.*

<table>
<thead>
<tr>
<th>TIME OF COLLECTION</th>
<th>RETENTION</th>
<th>DISPOSAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## DESCRIPTION OF SECURITY MEASURES

*State a general description of the organizational, physical, and technical security measures in place.*

<table>
<thead>
<tr>
<th>ORGANIZATIONAL</th>
<th>PHYSICAL</th>
<th>TECHNICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Policies

Collection

Storage

Transmission

Use

Retention

Disposal

Data Subject Rights

Security Measures

General Privacy Principles

ORGANIZATIONAL

PHYSICAL

TECHNICAL

Right to be Informed
Right to Access
Right to Object
Right to Rectification
Right to Erasure or Blocking
Right to Damages
Right to Data Portability
Right to File A Complaint

ORGANIZATIONAL

PHYSICAL

TECHNICAL

TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY
Risk Assessment Tools
Risk Assessment Tools
Risk Assessment Tools

- Accept
- Transfer
- Avoid
- Mitigate
- Organizational
  - Physical
  - Technical
PROGRAM CONTROLS

**Capacity Building**
Orientation or training programs regarding privacy

**Breach Handling**
Procedure and team responsible for managing data breaches

**PIP Management**
Vendor Management contractual provisions compliant with the Data Privacy Act
Compliance Framework &
Compliance Checks
Responsive Privacy Regulation

- Prosecute
  - Recommend Prosecution
- Enforce
  - Issue Compliance Orders (including temporary/permanent stop processing)
  - Impose Fines
  - Publish Case Studies
- Regulate
  - Conduct Compliance Checks
  - Update issuances
  - Receive complaints through Privacy Patrollers
  - Compliance Support Contact Center
    - PrivacyWall
    - PrivaHub
    - Publish monthly Tech Reports
  - Publish quarterly Compliance Checks Reports
  - Work with other regulators
Considerations for the Conduct of Compliance Checks

- **Level of risk** to the rights and freedoms of data subjects posed by personal data processing by a PIC or PIP;

- **Reports** received by the Commission against the PIC or PIP or its sector;

- **Non-registration** of a PIC or PIP that is subject to mandatory registration requirement as provided for under NPC Circular 17-01;

- **Unsecured** or publicly available personal data found on the internet that may be traced to a PIC or PIP; and

- **Other** considerations that indicate non-compliance with the DPA or the issuances of the Commission.
<table>
<thead>
<tr>
<th>Notices and Orders</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy Compliance Questionnaire (PCQ)</strong></td>
</tr>
<tr>
<td>- a document containing a series of questions formulated by the Commission to be answered by the PIC or PIP to contextualize documents and policies that the Commission requires to be submitted, and to evaluate the PIC/PIP’s compliance efforts</td>
</tr>
<tr>
<td><strong>Notice of Compliance Check (Notice of CC)</strong></td>
</tr>
<tr>
<td>- A PIC or PIP shall be notified of the conduct of a Compliance Check by the Commission</td>
</tr>
<tr>
<td>- Document Submission and On-site Visit</td>
</tr>
<tr>
<td><strong>Certificate of No Significant Findings (CNSF)</strong></td>
</tr>
<tr>
<td>- Issued when Compliance Check shows no substantial deficiencies without prejudice to the any recommendations for the improvement</td>
</tr>
<tr>
<td>- Issuance does not bar an investigation for any possible liability arising from complaints and/or personal data breaches</td>
</tr>
</tbody>
</table>
## Notices and Orders

<table>
<thead>
<tr>
<th>Notice of Deficiencies (NOD)</th>
<th>Compliance Order</th>
<th>Other Orders</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Issued if found to be non-compliant with certain obligations</td>
<td>■ Non-compliance persists after lapse of period in Notice of Deficiencies.</td>
<td>■ any and all pertinent orders in connection with the conduct or furtherance of any Compliance Check or the assessment of any organization’s compliance</td>
</tr>
<tr>
<td>■ indicating the required period of time within which to correct the identified deficiencies.</td>
<td>■ A report needs to be filed outlining actions taken.</td>
<td></td>
</tr>
<tr>
<td>■ A report needs to be filed outlining actions taken.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Compliance Checklist: Documents Submission

- Records of Processing Activities
- Privacy Impact Assessment
- Governance
- Policies and Procedures
- Data Security
- Breach Management
- 3rd Party (PIP) Management
## Compliance Checklist: On-site Visit

<table>
<thead>
<tr>
<th>Data Governance and Risk Assessment</th>
<th>Day to Day Privacy</th>
<th>Managing 3rd Party Risks</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration (NPC Circular 17-01)</td>
<td>Collection (IRR Sec 19 and 34)</td>
<td>Outsourcing Agreements (IRR Sec 43)</td>
<td>Breach Management (NPC Circular 16-03)</td>
</tr>
<tr>
<td>Governance (PMP)</td>
<td>Access and Use (IRR Sec 34)</td>
<td>Data Sharing Agreements (IRR Sec 20)</td>
<td>Continuing Assessment and Development</td>
</tr>
<tr>
<td>Management of Human Resources</td>
<td>Storage (NCP Circular 16-01)</td>
<td>Retention (IRR Sec 19)</td>
<td></td>
</tr>
<tr>
<td>(NPC Circular 16-01/16-03)</td>
<td>Transfer (NPC Circular 16-01 and IRR Sec 20 and 43)</td>
<td>Cross-border transfers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disposal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Outsourcing Agreements (IRR Sec 43)

Data Sharing Agreements (IRR Sec 20)

Cross-border transfers

Breach Management (NPC Circular 16-03)

Continuing Assessment and Development
Updates

Privacy Commission extends validity of registration until 2020

Personal Information Controllers (PICs) and Personal Information Processors (PIPs) that completed at least Phase-I of their registration with the National Privacy Commission (NPC) by 2018 are not required to renew their registration this year. The validity of their registration is extended until 8 March 2020.

They are also entitled to an official digital certificate of registration, available upon request with the NPC.

PICs and PIPs covered by NPC Circular 17-01 that have not yet registered are still required to register their Data Protection Officer to avoid possible liabilities. For instructions on how to comply with this requirement, please click this link.

For more details, refer to the FAQ page or contact us at:

Email Address: compliance@privacy.gov.ph
Phone Number: (02) 510-83-09
Mobile Number: +339451534299 TNT / +33965263419 TM

Notice to the Public

Personal Information Controllers and Processors who meet the conditions in §5 of NPC-Circular 17-01 shall register with the National Privacy Commission as part of the compliance requirements of the Data Privacy Act (2012) and its related issuances. If you have yet to register, please follow the procedure found on the following page.

For clarifications on any of the steps in the procedure, please consult our FAQs or email us at compliance@privacy.gov.ph.

REGISTER

- Government / Private institution
- Individual / Professional

FAQ

Downloadable Forms
Thank you!