The Data Privacy Act: Compliance and Accountability
Section 7.b

The National Privacy Commission has the power to...

• receive complaints,
• institute investigations,
• facilitate or enable settlement of complaints through the use of alternative dispute resolution processes,
• adjudicate,
• award indemnity on matters affecting any personal information,
• prepare reports on disposition of complaints and resolution of any investigation it initiates, and,
• in cases it deems appropriate, publicize any such report.
<table>
<thead>
<tr>
<th></th>
<th>Events that may trigger a data privacy investigation by the NPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Complaint from a data subject</td>
</tr>
<tr>
<td>02</td>
<td>Report from a whistle blower</td>
</tr>
<tr>
<td>03</td>
<td>Own Initiative</td>
</tr>
<tr>
<td>04</td>
<td>Random audit</td>
</tr>
</tbody>
</table>

The rules for complaints handling are contained in NPC Circular 16-04, “Rules of Procedure of the NPC”.

NPC does not reward whistle blowers.

May be based on a news article.

Sectoral
Nature Of Complaints received by NPC as of 30 June 2017

- Unauthorized Access/Breach Reports: 26%
- Consumer Protection: 14%
- Credit Card: 1%
- Cybercrime: 1%
- Drone: 1%
- Security of Personal Information: 20%
- Rights of Data Subject: 13%
- Unauthorized Disclosure: 5%
- General Inquiry: 12%
Complaints & Investigation Process

1. Data Subject submits written complaint to your organization.

2. If not settled, or not acted upon within 15 days, Data Subject may file sworn affidavit with NPC.

3. Other circumstances may trigger the NPC to conduct an investigation

4. After conducting its investigation, the NPC may:
   - Dismiss the case
   - Send it to arbitration
   - Find for complainant

Note: Findings are subject to appeal, which must be filed within 15 days.
If the complaint is upheld

The National Privacy Commission may...

- Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest (Sec. 7.c)
- Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy (Sec. 7.d)
- Recommend to the Department of Justice the prosecution and imposition of penalties specified in this Act (Sec. 7.i)
Who is liable? Who goes to jail?

- **Sec. 22.** The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein...

- **Sec. 34.** Extent of Liability. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.
The Obligations you must comply with

- Data Privacy Act of 2012
- IRRs (promulgated 2016)

2016 Series
- Circular 16-01 Gov’t Agencies
- Circular 16-02 Data Sharing
- Circular 16-03 Breach Mgmt
- Circular 16-04 Rules Procedure

2017 Series
- Advisory 17-01 DPO Guidelines
- Advisory 17-02 PDS Guidelines
- Advisory 17-03 PIA Guidelines
- Circular 17-01 Registration
<table>
<thead>
<tr>
<th>PUNISHABLE ACT</th>
<th>JAIL TERM</th>
<th>FINE (PESOS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access due to negligence</td>
<td>1y to 3y – 3y to 6y</td>
<td>500k to 4m</td>
</tr>
<tr>
<td>Unauthorized processing</td>
<td>1y to 3y – 3y to 6y</td>
<td>500k to 4m</td>
</tr>
<tr>
<td>Unauthorized purposes</td>
<td>18m to 5y – 2y to 7y</td>
<td>500k to 2m</td>
</tr>
<tr>
<td>Improper disposal</td>
<td>6m to 2y – 3y to 6y</td>
<td>100k to 1m</td>
</tr>
<tr>
<td>Intentional breach</td>
<td>1y to 3y</td>
<td>500k to 2m</td>
</tr>
<tr>
<td>Concealing breach</td>
<td>18m to 5y</td>
<td>500k to 1m</td>
</tr>
<tr>
<td>Malicious disclosure</td>
<td>18m to 5y</td>
<td>500k to 1m</td>
</tr>
<tr>
<td>Unauthorized disclosure</td>
<td>1y to 3y – 3y to 5y</td>
<td>500k to 2m</td>
</tr>
<tr>
<td>Combination of acts</td>
<td>3y to 6y</td>
<td>1m to 5m</td>
</tr>
</tbody>
</table>
Hypothetical Example: Database of Patients

Your hospital collects records of patients.

26 The Board decides that it’s more important to buy a new piece of equipment rather than protecting the data.

25 A nurse copies the database of asthma patients onto a USB and sells it to Drug Co.

32 Drug Co. uses the database for a marketing campaign to target patients for a radical new asthma treatment.

28 One of the patients who was contacted files a complaint with the hospital, and eventually elevates this complaint to the NPC.
DATA PRIVACY ACT OF 2012
How Can an Organization Comply?

STEP 1: Appoint a Data Protection Officer (DPO)

Personal information controllers and personal information processors are required to appoint or designate a data protection officer or compliance officer. DPOs will be accountable for ensuring compliance with applicable laws and regulations relating to data protection and privacy.

STEP 2: Conduct a Privacy Impact Assessment (PIA)

A Privacy Impact Assessment (PIA) is a process undertaken and used by a company or agency to evaluate and manage the impact of its program process and/or measure on data privacy.

STEP 3: Create Privacy Management Framework

Your Privacy Management Program serves to align everyone in the organization in the same direction, to facilitate compliance with Data Privacy Act and issuances of the NPC, and to help your organization in mitigating the impact of a data breach.

STEP 4: Implement Privacy and Data Protection Measures

The measures laid out in your privacy and data protection policies should not remain theoretical. They must continuously be assessed, reviewed, and revised as necessary, while training must be regularly conducted.

STEP 5: Exercise Breach Reporting Procedures

Upon the discovery of a personal data breach, or reasonable suspicion thereof, it is important to conduct an initial assessment of the breach, to mitigate its impact, and to notify both the affected data subjects and the National Privacy Commission (NPC) within 72 hours of discovery.

STEP 6: Register your company with the National Privacy Commission (NPC)

Registration with the NPC is up-to-date and contains all necessary compliance documentation. Registration includes all automated processing operations that would have legal effect on the data subject. Provide annual report which summarize documented security incidents and personal data breaches.

Contact:
Info@privacy.gov.ph
privacy.gov.ph
# 3-page Checklist

**Data Privacy Act (RA 10173) Checklist**

**Signs of Compliance, Commitment to Comply, Capacity to Comply** vs. **Signs of Negligence**

## Pillar 1: Commit to Comply: Appoint a Data Protection Officer (DPO)

Sec. 21 of the DPA, Section 50 of the IRR, Circular 16-01, and Advisory 17-01

<table>
<thead>
<tr>
<th>Appoint an individual accountable for compliance</th>
<th>Ineffective data protection governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Notarized designation of a DPO/COP, filed with the NPC</td>
<td>☐ No DPO or COP (in which case CEO or HoA is the default DPO)</td>
</tr>
<tr>
<td>☐ Evidence that DPO/COP recommendations are taken into consideration when making decisions</td>
<td>☐ Lack of interaction between DPO/COP and top management</td>
</tr>
<tr>
<td>☐ Contact details are easy to find (e.g. on website)</td>
<td>☐ Lack of interaction between DPO/COP and functional units</td>
</tr>
<tr>
<td>☐ Continuing education program for the DPO/COP</td>
<td>☐ Communication from the DPO/COP is largely ignored</td>
</tr>
<tr>
<td></td>
<td>☐ No continuing education program for the DPO/COP</td>
</tr>
</tbody>
</table>

## Pillar 2: Know Your Risks: Conduct a Privacy Impact Assessment (PIA)

Sec. 20(c) of the DPA, Section 29 of the IRR, Advisory 17-03

<table>
<thead>
<tr>
<th>Know the risks represented by the processing to the rights and freedoms of data subjects</th>
<th>Data processing controls do not take into account the risks to the rights and freedoms of data subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Up-to-date organizational inventory of processes that handle personal data, including the list of process owners</td>
<td>☐ No PIAs</td>
</tr>
<tr>
<td>☐ PIAs have been conducted, and are owned and kept up-to-date by the process owner</td>
<td>☐ Process owners do not “own” the PIAs</td>
</tr>
<tr>
<td>☐ Stakeholders (those involved in the information life cycle) have been consulted as part of the PIA process</td>
<td>☐ PIAs are not updated when changes are made to the process, or to the technologies being used in the process</td>
</tr>
<tr>
<td>☐ PIA includes a privacy risk map, a list of controls, an implementation plan, and a monitoring/evaluation milestone</td>
<td>☐ Stakeholders are not consulted for the PIA</td>
</tr>
<tr>
<td></td>
<td>☐ Controls identified during the PIA are not implemented</td>
</tr>
</tbody>
</table>
Compliance is a journey
Negligence is an abyss.

Compliance
Capacity to Comply
Commitment to Comply
Pillar 1: Commit to Comply:
Appoint a Data Protection Officer (DPO)
Legal Basis: Sec. 21 of the DPA, Section 50 of the IRR, Circular 16-01, and Advisory 17-01

<table>
<thead>
<tr>
<th>Ineffective data protection governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ No DPO or COP (in which case CEO or HoA is the default DPO)</td>
</tr>
<tr>
<td>☐ Lack of interaction between DPO/COP and top management</td>
</tr>
<tr>
<td>☐ Lack of interaction between DPO/COP and functional units</td>
</tr>
<tr>
<td>☐ Communication from the DPO/COP is largely ignored</td>
</tr>
<tr>
<td>☐ No continuing education program for the DPO/COP</td>
</tr>
</tbody>
</table>
Selecting a DPO for Healthcare Delivery

Minimum requirements

- business expertise
- knowledge of privacy principles
- empowered to be a change agent
- ideally, full-time
Support needed from Process Owners

- Process owners to own/maintain their respective Privacy Impact Assessments
- Process owners to consult on strategic projects involving the use of personal data (“Privacy by Design”)
- Process owners to conduct breach drills on their respective processes
Support needed from HR Team

- Roll-out training on privacy and data protection
- Issue security clearances to staff processing personal data. DPOs must have access to all security clearances issued.
- Implement the recommended organizational controls
Support needed from Legal

Legal to ensure that all PIP/service provider contracts, job orders, etc. are compliant. For example, all PIPs must also have their own DPO

Legal to ensure that all external sharing of data meets the required guidelines of the NPC
Support needed from Others

- IT to implement the recommended technical controls
- Security to implement the recommended physical controls
- Internal audit to test internally for compliance
Support needed from Top Management

- Budget support
- Incorporating compliance into the performance bonus parameters of those handling personal data
- Drive the message throughout the organization
Privacy Impact Assessment
Pillar 2: Know Your Risks: Conduct a Privacy Impact Assessment (PIA)
Legal Basis: Sec. 20(c) of the DPA, Section 29 of the IRR, Advisory 17-03

Sec. 20 (c) “The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation.”

How will you know what are “the risks represented by the processing”?

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Advisory No. 2017-03

DATE : 31 July 2017

SUBJECT : GUIDELINES ON PRIVACY IMPACT ASSESSMENTS

From https://privacy.gov.ph/advisories/
Summary: Steps in the PIA Process

1. Make an inventory of personal data held (including location and type of media)
2. Identify the projects, processes, programs, or measures that act on this data
3. Regularly review the list to determine whether a new/revised PIA is necessary
4. If a PIA is needed, plan and perform the assessment
5. Implement the control measures agreed upon
## PR / B * C = IA

### Example

<table>
<thead>
<tr>
<th>Program, Process, or Measure</th>
<th>Privacy Risk</th>
<th>Benefit</th>
<th>Controls</th>
<th>Impact Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.1</td>
<td>High</td>
<td>Low</td>
<td></td>
<td>Unacceptable</td>
</tr>
<tr>
<td>X.2</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Unreasonable</td>
</tr>
<tr>
<td>X.3</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Acceptable</td>
</tr>
<tr>
<td>X.25</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Acceptable</td>
</tr>
</tbody>
</table>
Pillar 2: Know Your Risks: Conduct a Privacy Impact Assessment (PIA)
Legal Basis: Sec. 20(c) of the DPA, Section 29 of the IRR, Advisory 17-03

| Know the risks represented by the processing to the rights and freedoms of data subjects |
| Data processing controls do not take into account the risks to the rights and freedoms of data subjects |
| ☐ No PIAs |
| ☐ Process owners do not "own" the PIAs |
| ☐ PIAs are not updated when changes are made to the process, or to the technologies being used in the process |
| ☐ Stakeholders are not consulted for the PIA |
| ☐ Controls identified during the PIA are not implemented |
### Pillar 3: Write Your Plan: Create Your Privacy Management Program

**Legal Basis:** Sec. 11-15 of the DPA, Sections 21-23 and 43-45 of the IRR, Circulars 16-01 and 16-02

#### Processing of data is according to privacy principles of transparency, legitimate purpose, and proportionality

Data processing not according to privacy principles of transparency, legitimate purpose, and proportionality:

- [ ] Processing fails to meet the criteria for lawful processing of personal data
- [ ] No privacy policy
- [ ] Privacy policy exists, but is not cascaded throughout the organization
- [ ] No privacy training or security clearance for data handlers
- [ ] Data is being shared without data sharing agreements
- [ ] No records of data processing
Be sure to read...

**Section 12** – Conditions under which processing Personal Information is ALLOWED...

**Section 13** – Processing of Sensitive Personal Information is PROHIBITED except in the following cases...
Do you share data?

Are you providing ACCESS to personal data you have collected to a third party, e.g. PhilHealth?

Is there a specific provision of LAW that specifically requires data sharing?

If there is no specific provision of law, is there a public service and a STATUTORY MANDATE? Do you have CONSENT of the data subject?
What’s in a DSA?

- Purpose of Data Sharing, including the Public Function and Public Service it facilitates
- Parties to the agreement (usually 2 or more PICs)
- Term or Duration of the Agreement
- Overview of operational details and general description of security measures
- How data subjects can exercise their rights
Pillar 4: Be Accountable: Implement your Privacy & Data Protection (PDP) Measures

Legal Basis: Sec. 16-18 and 38 of the DPA, Sections 17-24 and 34-37 of the IRR, Circular 16-04

<table>
<thead>
<tr>
<th>Upholding the rights of data subjects</th>
<th>Neglecting the rights of data subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Data subjects are apprised of their rights through a privacy notice</td>
<td>□ No privacy notice when collecting personal data</td>
</tr>
<tr>
<td>□ Consent is obtained prior to the collection and processing of data</td>
<td>□ Consent is not obtained prior to the collection/processing of data</td>
</tr>
<tr>
<td>□ Data subjects are provided a means to access their data</td>
<td>□ No venue for data subjects to access their data</td>
</tr>
<tr>
<td>□ Data subjects are provided a venue to correct/rectify their data</td>
<td>□ No venue for data subjects to correct/rectify their data</td>
</tr>
<tr>
<td>□ Data subjects know who to complain to if their rights are violated</td>
<td>□ No contact details on how to lodge a complaint</td>
</tr>
<tr>
<td>□ Complaints are acted upon quickly (within 30 days)</td>
<td>□ Complaints take a long time to be remedied</td>
</tr>
<tr>
<td>□ These rights are upheld when invoked by the lawful heirs or assigns of the data subject</td>
<td>□ Inaction on complaints from data subjects</td>
</tr>
<tr>
<td>□ Overcollection of personal data</td>
<td></td>
</tr>
</tbody>
</table>
Sec. 16-18
Rights of Data Subjects

✓ Right to be informed
✓ Right to object
✓ Right to access
✓ Right to correct/rectify
✓ Right to block/remove
✓ Right to data portability
✓ Right to file a complaint
✓ Right to be indemnified
**Pillar 4: Be Accountable: Implement your Privacy & Data Protection (PDP) Measures**

**Legal Basis:** Sec. 20, 22 and 24 of the DPA, Sections 25-29 of the IRR, Circular 16-01 and Health Privacy Code

<table>
<thead>
<tr>
<th>Maintaining confidentiality, integrity, and availability</th>
<th>Insufficient controls to maintain confidentiality, integrity, and availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Data protection risks have been identified and documented</td>
<td>□ Controls for data protection are not appropriate for the risks identified</td>
</tr>
<tr>
<td>□ Appropriate and up-to-date organizational, physical, and technical controls are in place to manage these risks (e.g ISO/IEC 27002)</td>
<td>□ Controls for data protection are not updated for new risks/threats</td>
</tr>
<tr>
<td>□ Data protection policies are cascaded throughout the organization and updated as needed</td>
<td>□ Controls for data protection are not complied with</td>
</tr>
<tr>
<td>□ Vulnerability scanning is conducted at least once a year</td>
<td>□ Cyber-hygiene practices are lax</td>
</tr>
<tr>
<td>□ Business continuity drills are conducted at least once a year</td>
<td>□ Business continuity drill has not been conducted in the last 12 months</td>
</tr>
<tr>
<td>□ For data stored outside the Philippines, location of foreign country is defined</td>
<td>□ Security vulnerability scanning has not been conducted in the last 12 months</td>
</tr>
<tr>
<td>□ For personal data stored in the cloud, NPC recommends that provider is ISO/IEC 27018 compliant (from Circular 16-01)</td>
<td></td>
</tr>
<tr>
<td>□ For digitized personal data, NPC recommends 256-bit AES for data at rest and in transit (from Circular 16-01)</td>
<td></td>
</tr>
</tbody>
</table>
Pillar 4: Be Accountable: Implement your Privacy & Data Protection (PDP) Measures

- **SEC. 20 (a)** The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful *destruction, alteration and disclosure*, as well as against any other unlawful processing.

- Guard against: **Destruction, Alteration, Disclosure**
- Objective/Goal: Availability, Integrity, Confidentiality (CIA)
- Measures: Organizational, Physical, Technical
Pillar 5: Be Prepared: Regularly exercise your Breach Reporting Procedures

Legal Basis: Sec. 20.f and 30 of the DPA, Sections 38-42 and 57 of the IRR, Circular 16-03

IRR Sec. 38 (a) The Commission and affected data subjects shall be notified by the PIC within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred.

From https://privacy.gov.ph/memorandum-circulars/
Pillar 5: Be Prepared: Regularly exercise your Breach Reporting Procedures

Legal Basis: Sec. 20.f and 30 of the DPA, Sections 38-42 and 57 of the IRR, Circular 16-03

<table>
<thead>
<tr>
<th>Able to report breach within 72 hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Forma of a data breach response team with clearly defined roles and responsibilities</td>
</tr>
<tr>
<td>0 Clearly defined and up-to-date incident response procedure</td>
</tr>
<tr>
<td>0 Breach drills are conducted at least once a year</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unable/unwilling to report breach within 72 hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 No breach response team</td>
</tr>
<tr>
<td>0 No breach response policy or procedures</td>
</tr>
<tr>
<td>0 Breach drill has not been conducted in the last 12 months</td>
</tr>
<tr>
<td>0 No notification of the NPC within 72 hours of discovery of a breach of personal data (possible criminal offense)</td>
</tr>
</tbody>
</table>
Recommendations (Circular 16-03, Sec. 4 and 5)

Form a data breach response team

• Led by an executive empowered to make immediate decisions.
• Should include someone familiar with the privacy impacts (PIA) of the data that has been breached.
• May include PR, HR, DPO, IT, service providers, Legal, Security
• Mandated to comply with the NPC’s reporting requirements.
• Functions may be outsourced, but not the role.

Create a security incident management policy

• Mandates creation of a breach team.
• Lays out measures to prevent or minimize data breaches.
• Ensures timely discovery and identification of security incidents that could result in a data breach.
• Implements an incident response procedure to contain the breach, restore system integrity, and mitigate possible harm and negative consequences to the data subject.
When is notification required?
Circular 16-03, Section 11

01
The personal data involves sensitive information, or any other information that may be used to enable identity fraud.

02
There is reason to believe that the information may have been acquired by an unauthorized person.

03
The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.
Notification of NPC
Circular 16-03, Section 17

Contents of Notification

- Nature of the Breach, Personal Data Involved
- Remedial Measures to Address Breach and Harmful Consequences
- Contact Person/s

Form of Notification

- Submission to CID of NPC: Written or electronic (complaints@privacy.gov.ph)
- Ensure that the NPC confirms receipt of notification

Deadline for Notification

- Within 72 hours upon knowledge of or reasonable belief that a personal data breach has occurred
Notification of Data Subjects
Circular 16-03, Section 18-19

Procedure for Notification of Data Subjects

- Within 72 hours of the breach, data subjects must be individually informed, in written or electronic form, about the nature of the breach and the data involved, measures taken to address the breach and reduce the consequences, contact person/s and any assistance to be provided.

Factors that may be considered in exempting notification

- Implementation of security measures that would prevent use of the data
- Measures taken to ensure that negative consequence will not materialize
- Age or legal capacity of affected data subjects

Factors that the NPC must be consulted on

- Notification is not reasonably possible within the prescribed period
- Notification would not be in the public interest or in the interest of the affected data subjects
- Notification may hinder the progress of a criminal investigation

NATIONAL PRIVACY COMMISSION
Summary: What compliance looks like

1. Registration with the NPC by March 8, 2018
2. Privacy impact assessments ASAP, conducted by the process owners
3. Breach team and procedures in place ASAP, after conduct of PIA
4. Privacy policies and data protection measures ASAP, disseminated within the organization
5. PIP contracts / data sharing agreements ASAP, with assistance from Legal
6. Notification to NPC within 72 hours ASAP, in the event of a personal data breach
NATIONAL PRIVACY COMMISSION

doing what's required

doing what's necessary

COMPLIANCE

ACCOUNTABILITY
I brush my teeth after every meal, as required. I do what’s needed to make sure I have no cavities and my breath is fresh all the time.
Don’t just comply.

Be accountable!

Thank You!

For joining us in building a culture of privacy.