Primer on the Data Privacy Act (DPA) of 2012
ABCD-S: "Awareness, Breach Management, Compliance, Data Protection Officer and Security Measures"

Dr. Rolando R. Lansigan
Chief, Compliance and Monitoring Division
National Privacy Commission (NPC)
Do not COLLECT if you cannot PROTECT
BOTPA
Who stores data about you?
SPEED OF INFORMATION

- 701,389 Facebook logins
- 20.8 MILLION+ Messages
- 150 MILLION Emails Sent
- 1,389 Uber Rides
- 527,760 Photos Shared
- 51,000 App Downloads From Apple
- 69,444 Hours watched
- 2.78 MILLION Video Views
- 2.4 MILLION Search Queries
- $203,596 In sales
- 38,052 Hours of Music
- 1.04 MILLION Vine Loops
- 38,194 Posts to Instagram
- 347,222 New Tweets
- 120+ New LinkedIn Accounts
- 60 SECONDS
Which is more valuable?

Data

Money
“Data is more valuable than Money. If someone takes your money, that's all they have. If you let someone take your data, they may eventually take your money too!“

from: Deputy Privacy Commissioner Dondi Mapa
In today’s environment, where competitors can copy your products, pirate your employees, and mirror your algorithms, **data** is the only sustainable competitive advantage.

FORMER DEPUTY PRIVACY COMMISSIONER DAMIAN MAPA
What is the Data Privacy Act of 2012?

- SECTION 1. Short Title. – This Act shall be known as the “Data Privacy Act of 2012”.

- Republic Act 10173, the Data Privacy Act of 2012

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

- The National Privacy Commission (NPC) is a body that is mandated to administer and implement this law. The functions of the NPC include:
  – rule-making,
  – advisory,
  – public education,
  – compliance and monitoring,
  – investigations and complaints,
  – and enforcement.
Main Author of R.A. 10173 and the NPC Commissioners
Data Privacy Act (DPA) Passed into law

National Privacy Commission (NPC) was formed

Implementing rules and Regulations (IRRs) was published

IRRs came into effect (comply with all provisions except registration requirements)

Comply with registration requirements

Registration Requirements: All personal data processing systems (DPS) operating in the Philippines that involve Personally Identifiable Information (PII) concerning at least 1,000 individuals/personal records must be registered with NPC

12 months
KEY ROLES IN THE DATA PRIVACY ACT

• **Data Subjects**
  - Refers to an individual whose, sensitive personal, or privileged information is processed personal

• **Personal Information Controller (PIC)**
  - Controls the processing of personal data, or instructs another to process personal data on its behalf.

• **Personal Information Processor (PIP)**
  - Organization or individual whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject

• **Data Protection Officer (DPO)**
  - Responsible for the overall management of compliance to DPA

• **National Privacy Commission**
  - Independent body mandated to administer and implement the DPA of 2012, and to monitor and ensure compliance of the country with international standards set for personal data protection
Examples of Breaches

1. COMELeak (1 and 2)
2. BPI – consent form
3. Hospital in Visayas – unsecure disposal of records (physical and digital)
4. Student transferred by her parent without her knowledge
5. Clinical record of a student to disclose with her parents?
6. List of top students/passers
7. Known Fastfood delivery – disclosing personal info of clients
8. Data sharing agreement (DSA) between and among Schools and Universities
9. Cedula in malls
10. Security issues in buildings – logbook
11. Profiling of customers from a mall
12. Unjustifiable collection of personal data of a school
13. Privacy notice
14. Use of USB
15. Personal laptop stolen
16. Lost a CD in transit
17. An error in viewing of student records in the online system
18. Use of re-cycled papers
19. Raffle stubs
20. Universities and Colleges with weak authentication
21. Personal Records stolen from home of an employee
22. Photocopiers re-sold without wiping the hard drives
23. Hacker attack on vulnerabilities
24. Hard drives sold online
25. Password hacked/revealed
26. Unencrypted Data
27. Personal laptop stolen
In the event of a data breach, we will not ask you how many millions you’ve spent on your hardware and IT experts.

We will, instead, ask whether you’ve implemented **NPC’s five data privacy guidelines**.
<table>
<thead>
<tr>
<th>DPA Section</th>
<th>Punishable Act</th>
<th>For Personal Information</th>
<th>For Sensitive Personal Information</th>
<th>Fine (Pesos)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>JAIL TERM</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Unauthorized processing</td>
<td>1-3 years</td>
<td>3-6 years</td>
<td>500 k – 4 million</td>
</tr>
<tr>
<td>26</td>
<td>Access due to negligence</td>
<td>1-3 years</td>
<td>3-6 years</td>
<td>500 k – 4 million</td>
</tr>
<tr>
<td>27</td>
<td>Improper disposal</td>
<td>6 months – 2 years</td>
<td>3-6 years</td>
<td>100 k – 1 million</td>
</tr>
<tr>
<td>28</td>
<td>Unauthorized purposes</td>
<td>18 months – 5 years</td>
<td>2-7 years</td>
<td>500 k – 2 million</td>
</tr>
<tr>
<td>29</td>
<td>Intentional breach</td>
<td></td>
<td>1-3 years</td>
<td>500 k – 2 million</td>
</tr>
<tr>
<td>30</td>
<td>Concealment of breach</td>
<td></td>
<td>18 months – 5 years</td>
<td>500 k – 1 million</td>
</tr>
<tr>
<td>31</td>
<td>Malicious disclosure</td>
<td></td>
<td>18 month – 5 years</td>
<td>500 k – 1 million</td>
</tr>
<tr>
<td>32</td>
<td>Unauthorized disclosure</td>
<td>1-3 years</td>
<td>3-5 years</td>
<td>500 k – 2 million</td>
</tr>
<tr>
<td>33</td>
<td>Combination of acts</td>
<td></td>
<td>1-3 years</td>
<td>1 million – 5 million</td>
</tr>
<tr>
<td>Rank</td>
<td>Fined entity</td>
<td>Amount of fines and penalties</td>
<td>Year</td>
<td>Country</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------</td>
<td>------------------------------</td>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>1</td>
<td>Apple</td>
<td>$32.5M</td>
<td>2014</td>
<td>U.S.</td>
</tr>
<tr>
<td>2</td>
<td>Google</td>
<td>$22.5M</td>
<td>2012</td>
<td>U.S.</td>
</tr>
<tr>
<td>3</td>
<td>Google</td>
<td>$17M</td>
<td>2013</td>
<td>U.S.</td>
</tr>
<tr>
<td>4</td>
<td>ChoicePoint</td>
<td>$15M</td>
<td>2006</td>
<td>U.S.</td>
</tr>
<tr>
<td>5</td>
<td>Hewlitt-Packard</td>
<td>$14.5M</td>
<td>2006</td>
<td>U.S.</td>
</tr>
<tr>
<td>6</td>
<td>LifeLock</td>
<td>$12M</td>
<td>2010</td>
<td>U.S.</td>
</tr>
<tr>
<td>7</td>
<td>TJ Maxx</td>
<td>$9.8M</td>
<td>2009</td>
<td>U.S.</td>
</tr>
<tr>
<td>8</td>
<td>Dish Network</td>
<td>$6M</td>
<td>2009</td>
<td>U.S.</td>
</tr>
<tr>
<td>9</td>
<td>DirecTV</td>
<td>$5.3M</td>
<td>2005</td>
<td>U.S.</td>
</tr>
<tr>
<td>10</td>
<td>HSBC</td>
<td>$5M</td>
<td>2009</td>
<td>UK</td>
</tr>
<tr>
<td>12</td>
<td>Craftmatic</td>
<td>$4.3</td>
<td>2007</td>
<td>U.S.</td>
</tr>
<tr>
<td>13</td>
<td>Cignet Health</td>
<td>$4.3M</td>
<td>2011</td>
<td>U.S.</td>
</tr>
<tr>
<td>14</td>
<td>Barclays Bank</td>
<td>$3.8M</td>
<td>2013</td>
<td>U.S.</td>
</tr>
<tr>
<td>15</td>
<td>Certegy Check Services</td>
<td>$3.5M</td>
<td>2013</td>
<td>U.S.</td>
</tr>
<tr>
<td>16</td>
<td>Playdom</td>
<td>$3M</td>
<td>2011</td>
<td>U.S.</td>
</tr>
<tr>
<td>17</td>
<td>The Broadcast Team</td>
<td>$2.8M</td>
<td>2007</td>
<td>U.S.</td>
</tr>
<tr>
<td>18</td>
<td>Equifax, TransUnion and Experian</td>
<td>$2.5M</td>
<td>2000</td>
<td>U.S.</td>
</tr>
<tr>
<td>19</td>
<td>CVS Caremark</td>
<td>$2.3M</td>
<td>2009</td>
<td>U.S.</td>
</tr>
<tr>
<td>20</td>
<td>Norwich Union Life</td>
<td>$1.8M</td>
<td>2007</td>
<td>UK</td>
</tr>
</tbody>
</table>

**SOURCE IAPP  17 FEB 2014**
Rights of the Data Subject

- Right to be informed - IRR, Section 34.a
- Right to object - IRR, Section 34.b
- Right to access - IRR, Section 34.c
- Right to data portability - IRR, Section 36
- Right to correct (rectification) - IRR, Section 34.d
- Right to erasure or blocking - IRR, Section 34.e
- Right to file a complaint - IRR, Section 34.a.2
- Right to damages - IRR, Section 34.f
- Right to transmissibility - IRR, Section 35
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.
<table>
<thead>
<tr>
<th>Personal Information</th>
<th><strong>Sensitive Personal Information</strong> (List based on IRR)</th>
<th><strong>Privileged Information</strong> (List based on Rules of Court)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Race</td>
<td>Data received within the context of a protected relationship – husband and wife</td>
</tr>
<tr>
<td>Address</td>
<td>Ethnic origin</td>
<td></td>
</tr>
<tr>
<td>Place of work</td>
<td>Marital status</td>
<td></td>
</tr>
<tr>
<td>Telephone number</td>
<td>Age</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>Color</td>
<td></td>
</tr>
<tr>
<td>Location of an individual at a particular time</td>
<td>Religious affiliation</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>Philosophical affiliation</td>
<td></td>
</tr>
<tr>
<td>Birth date</td>
<td>Political affiliation</td>
<td></td>
</tr>
<tr>
<td>Birth place</td>
<td>Health</td>
<td></td>
</tr>
<tr>
<td>Country of citizenship</td>
<td>Education</td>
<td></td>
</tr>
<tr>
<td>Citizenship status</td>
<td>Genetics</td>
<td></td>
</tr>
<tr>
<td>Payroll &amp; benefits information</td>
<td>Sexual life</td>
<td></td>
</tr>
<tr>
<td>Contact information</td>
<td>Proceeding for any offense committed or alleged to have been committed, the disposal of such proceedings, the sentence of any court in such proceedings</td>
<td>Data received within the context of a protected relationship – doctor and patient</td>
</tr>
<tr>
<td>Sensitive Personal Information (List based on IRR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social security number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licenses or its denials, suspension or revocation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tax returns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other personal info issued by government agencies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank and credit/debit card numbers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Websites visited</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Materials downloaded</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any other information reflecting preferences and behaviors of an individual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grievance information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discipline information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leave of absence reason</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licenses or its denials, suspension or revocation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Personal Data Lifecycle

Acquisition → Storage → USE

Transfer → Destruction

Key considerations when listing your personal data:
- What personal data do you collect?
- In what form and through which channels?
- For what purpose do you collect personal data?
- How is it used?
- Who is this data shared with internally and externally?
- Who is authorized to access this data?
- Where do you keep your data?
- How long do you keep your data?
- How do you dispose of this data?

Retention/Disposal should be based on:
1. Law
2. Industry Best Practice
3. Business Needs
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.
**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.
Please be advised:

Your voice and appearance may be recorded while you are visiting the [REDACTED] today. By entering, you are granting [REDACTED] and its partners permission to use your recorded likeness in all media, in perpetuity.

Thank you.
**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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permanent Address</td>
<td>*(Permanent) Region - region - (Permanent) Province - province - (Permanent) Municipality - municipality - Zip Code</td>
</tr>
<tr>
<td>Residential Tel No.</td>
<td>Phone Number:</td>
</tr>
<tr>
<td>Provincial Address</td>
<td>*(Provincial) Region - region - (Provincial) Province - province - (Provincial) Municipality - municipality -</td>
</tr>
<tr>
<td>Provincial Tel No.</td>
<td></td>
</tr>
<tr>
<td>Height (in feet and inches)</td>
<td></td>
</tr>
<tr>
<td>Weight (in pounds)</td>
<td></td>
</tr>
<tr>
<td>Learner Reference Number (LRN)</td>
<td></td>
</tr>
<tr>
<td>QVR</td>
<td></td>
</tr>
<tr>
<td>indigenous People</td>
<td></td>
</tr>
<tr>
<td>Mother Tongue</td>
<td></td>
</tr>
<tr>
<td>Email Address</td>
<td></td>
</tr>
<tr>
<td>Facebook Account</td>
<td></td>
</tr>
<tr>
<td>Personal Website</td>
<td></td>
</tr>
<tr>
<td>Is Working Student</td>
<td></td>
</tr>
</tbody>
</table>

**FAMILY DATA**

| Father's Name                              | Occupation - selected occupation -                   |
| Contact Number                             |                                                        |
| Mother's Name                              |                                                        |
| Contact Number                             |                                                        |
| Birth Rank                                 | only child eldest middle youngest                     |
| Parent's Home Address                      |                                                        |
| No. of Siblings                            |                                                        |
| Living Condition                           |                                                        |
| Who's financing your education?            |                                                        |
| Living Arrangement                         |                                                        |
**No. of Siblings**
\[\text{No. of Siblings}\]

**No. of Brothers**
\[\text{No. of Brothers}\]

**Brother(s) With Income**
\[\text{Brother(s) With Income}\]

**If married, name of spouse**
\[\text{If married, name of spouse}\]

**Occupation**
\[\text{Occupation}\]

**Annual Family Income**
\[\text{Annual Family Income}\]

**Persons to be notified in case of emergency**

<table>
<thead>
<tr>
<th>Guardian’s Name</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guardian’s Tel No</td>
<td>Guardian’s Cell #</td>
</tr>
</tbody>
</table>

**Educational Data**

<table>
<thead>
<tr>
<th>School Level</th>
<th>School Type</th>
<th>Name of School</th>
<th>Address</th>
<th>Grade / Program</th>
<th>Year Attended</th>
<th>Honors/Awards Received</th>
<th>General Average</th>
</tr>
</thead>
</table>

**Other Information**

<table>
<thead>
<tr>
<th>Award/Talent</th>
<th>Organization Membership</th>
<th>Work Experience</th>
<th>Place of Work</th>
<th>Inclusive Date</th>
</tr>
</thead>
</table>

**For Foreign Student Only**

<table>
<thead>
<tr>
<th>Passport No.</th>
<th>Date Issued</th>
<th>Place Issued</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type Of Visa</td>
<td>Visa Status</td>
<td>I-Card No.</td>
</tr>
</tbody>
</table>

**Remarks**
\[\text{Remarks}\]
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).
Other Requirements

- Annual Breach Drill
  - Notification to NPC within 72 hours
  - (in the event of a personal data breach)
- Annual Breach Report
- Security Clearance
- Privacy Notice
- Data Sharing Agreement (DSA), if applicable
- Sub-contracting Agreement / Outsourcing Agreement

Privacy notice

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?

Data sharing checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis.

Is the sharing justified?
Key points to consider:
- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?
Key points to consider:
- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:
- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.
The Data Privacy Principles

• Personal data shall be:
  1. processed fairly and lawfully
  2. processed only for specified, lawful and compatible purposes
  3. adequate, relevant and not excessive
  4. accurate and up to date
  5. kept for no longer than necessary
  6. processed in accordance with the rights of data subjects
  7. kept secure
  8. shared to other PICs only if there is a DSA.
Self-help checklist on data protection policy

Remember: you should be able to answer **YES** to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don’t have a clean sheet, the checklist can help you identify the areas where you need to improve.

Rule 1: Fair obtaining:
- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them?
- Can we describe our data-collection practices as open, transparent and up-front?

Rule 2: Purpose specification
- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?
- If we are required to register with NPC, does our register entry include a proper, comprehensive statement of our purpose? [Remember, if you are using personal data for a purpose not listed on your register entry, you may be committing an offence.]
- Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?
Self-help checklist on data protection policy

Remember: you should be able to answer **YES** to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

**Rule 3: Use and disclosure of information**

- Are there defined rules about the use and disclosure of information?
- Are all staff aware of these rules?
- Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.
- If we are required to register with NPC, does our register entry include a full list of persons to whom we may need to disclose personal data? *Remember, if you disclose personal data to someone not listed on your register entry, you may be committing an offence.*

**Rule 4: Security**

- Is there a list of security provisions in place for each data set?
- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data we keep?
- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files securely locked away from unauthorized people?
Self-help checklist on data protection policy

Remember: you should be able to answer **YES** to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

**Rule 5: Adequate, relevant and not excessive**
- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard?

**Rule 6: Accurate and up-to-date**
- Do we check our data for accuracy?
- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?
Self-help checklist on data protection policy

Remember: you should be able to answer YES to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

Rule 7: Retention time
• Is there a clear statement on how long personal data are to be retained?
• Are we clear about any legal requirements on us to retain data for a certain period?
• Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?
• Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Rule 8: The Right of Access
• Is a named individual responsible for handling access requests?
• Are there clear procedures in place for dealing with such requests?
• Do these procedures guarantee compliance with the RA 10173 requirements?
Self-help checklist on data protection policy

Remember: you should be able to answer **YES** to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

**Registration**
- Are we clear about whether or not we need to be registered with the NPC?
- If registration is required, is the registration kept up to date? Does the registration accurately reflect our practices for handling personal data? [Remember, if your data-handling practices are out of line with the details set out in your register entry, you may be committing an offence.]

**Training & Education**
- Do we know about the levels of awareness of data protection in our organization?
- Are our staff aware of their data protection responsibilities - including the need for confidentiality?
- Is data protection included as part of the training program for our staff?
Self-help checklist on data protection policy

Remember: you should be able to answer **YES** to all of the questions below. If you can, your business is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

Co-ordination and Compliance

- Has a Data Protection Officer (DPO) / Compliance Officer for Privacy (COP) been appointed?
- Are all staff aware of his or her role?
- Are there mechanisms in place for formal review by DPO activities within our organization?
- Is the Privacy Impact Assessment (PIA) carefully planned and executed according to its purpose?
- Is there a Breach Management Program (BMP) in place?

Other Requirements

- Annual Breach Drill
  - **Notification to NPC within 72 hours** *(in the event of a personal data breach)*
- Annual Breach Report
- Security Clearance
- Privacy Notice
- Data Sharing Agreement (DSA), if applicable
- Sub-contracting Agreement / Outsourcing Agreement
1 Technical

2 Organisational – other measures
Encryption
To what standard? (cost Vs benefit)
All devices or just some?

Passwords
Enforced strength and updates?

Sharing data
Technical solutions – e.g. via email; portals

System testing & maintenance
Who has access, to what (System Administrators)
Live or dummy data?

Backups
Secure: encrypted tapes | cloud-provider
Auditable process

Access control
Who decides permissions and privileges (‘need to know’)?

Remote access
How delivered securely?
Permit Bring Your Own Device?
**Organisational – physical security**

### Secure Office Storage
- For removable devices and hardcopy information
  - Identifying marks?
  - Locked print?
  - Kensington locks?
  - Offsite?

### Remote working
- Secure both hardcopies and devices when in transit.
- Kept out of sight: in transit | at home.
- Lockable pedestals | Kensington locks?

### Building access control
- Secure premises – CCTV | locked windows | perimeter
  - Locked CCTV room | server room
  - ID badges, supervised visitors | contractors

### Secure disposal
- Shredding of hardcopies
- Beyond use | Reuse | Resale
Organisational – other measures

Policy, procedures, guidance & training

- Eliminate ambiguities
- Clearly communicated, readily accessible and understood

Human Resources

- Explicit roles and responsibilities in Job Descriptions and Terms of Reference
- Terms and Conditions: confidentiality clauses
- Clear expectations | reporting lines

Procurement (and contracts)

- i.e. outsourced services like IT and software
- Due diligence
- Compliant contract Terms and Conditions:
  - Act on your instructions
  - Equivalent security
- Auditing and monitoring

Disciplinary process

Training records
# Registration of Data Processing System

**Data Protection Officer (DPO)**

Note: The personal information submitted herein shall be used for the initial phase of the Data Processing System Online Registration and supporting documents should be attached along with this form. Once this form has been validated by the NPC, you will be given an access code via email and SMS to continue with your registration with the online system. You may find the list of supporting documents in our guidelines emailed to you via email and posted on our website.

## Personal Information Controller

<table>
<thead>
<tr>
<th>Name of the Organization</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website (URL)</td>
<td>Tel. No.</td>
</tr>
<tr>
<td>Company Address</td>
<td></td>
</tr>
<tr>
<td>Role/Position</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Tel. No.</th>
<th>Mobile No.</th>
<th>Official Designation</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Permanent: 1971</td>
</tr>
</tbody>
</table>

## Sworn Statement

I declare under oath that this Registration Form is accomplished by Data Protection Officer, and is a true, correct and complete statement and pursuant to the provisions of the pertinent laws, rules and regulations of the Republic of the Philippines. I also authorize the National Privacy Commission to verify the contents stated herein.

Head of Agency (Signature/Printed Name)

Data Protection Officer (Signature/Printed Name)

Authorized as SWORN to before me, the ______________, who exhibited to me (either) Government Issued ID Yes / No

Issued on ____________

Notary Public

**To be filled by NPC Compliance and Monitoring Division**

<table>
<thead>
<tr>
<th>Code</th>
<th>Signed/Approved by (Signature/Printed Name)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date (MM/DD/YYYY)</td>
</tr>
</tbody>
</table>
Designating a DPO is the first essential step. You cannot register with the NPC unless you have a DPO.
General Qualifications

• The Data Protection Officer (DPO) should possess specialized knowledge and demonstrate reliability necessary for the performance of his or her duties and responsibilities. As such, the DPO should have expertise in relevant privacy or data protection policies and practices. He or she should have sufficient understanding of the processing operations being carried out by the Personal Information Controller (PIC) or the Personal Information Processor (PIP), including the latter’s information systems, data security and/or data protection needs.

• Knowledge by the DPO of the sector or field of the PIC or PIP, and the latter’s internal structure, policies, and processes is also useful.

• The minimum qualifications for a DPO shall be proportionate to his or her functions.
Duties and Responsibilities Of the DPO

a. monitor the PIC’s or PIP’s compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:

1. collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;

2. analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;

3. inform, advise, and issue recommendations to the PIC or PIP;

4. ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and

5. advice the PIP or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;
b. ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;

c. advice the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);

d. ensure proper data breach and security incident management by the PIC or PIP, including the latter’s preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;

e. inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;
f. advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;

g. serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;

h. cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and

i. perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.
Additional functions of a Data Protection Officer (DPO):

1. ensuring that controllers and data subjects are informed of their rights and obligations;
2. ensuring in an independent manner the internal application of the Regulation;
3. carrying out inquiries where necessary;
4. keeping a register of the processing operations carried out by the controller;
5. notifying the NPC of processing operations which may present specific risks;
6. responding to requests from NPC and cooperating with NPC.
What support is needed from the rest of the org’n?

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”)
- Breach Drill to be conducted regularly test each Privacy Impact at least once a year
What support is needed from the rest of the org’n?

From HR

- Roll-out training on privacy and data protection
- Issue security clearances to staff processing personal data (such clearance to be made contingent on passing the privacy training). DPOs must have access to all security clearances issued.
- Implement the recommended organizational controls
What support is needed from the rest of the org’n?

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.

Note: In order to avoid “privilege” issues, it’s not advisable to have legal counsel be the DPO.
What support is needed from the rest of the org’n?

From Other Support Teams

- IT to implement the recommended technical controls
- Security to implement the recommended physical controls
- Internal audit to test internally for compliance
What support is needed from the rest of the org’n?

**From Top Management**

- Budget support for security controls (technical, organizational, physical), for compliance tools and technology, for informational and training activities, for consultants, external auditors, advisors
- Incorporating compliance into the performance bonus parameters of those concerned, especially for those handling personal data
- Drive the message throughout the organization
- Drive the urgency (e.g. like the SARS epidemic, when everyone started installing hand sanitizers)
In Closing: How the NPC can help

- Help in delivering the message to top management
- Generic guidance and frameworks (www.privacy.gov.ph)
- Updates on new standards and/or circulars (www.privacy.gov.ph)
- When requested, advice on specific matters (info@privacy.gov.ph)
“Compliance to Data Privacy Act is not a one-shot initiative. It is a discipline and culture that must be embedded on a continuous basis within the organization.”

CULTURE OF PRIVACY in the PHILIPPINES
Thank you! Any questions?

info@privacy.gov.ph