“THE PRIVACY LAW AND IMPACT ON PRIVATE HEALTH CARE PROVIDERS”

Raymund E. Liboro
Privacy Commissioner and Chairman
Forbes Most Valuable Brands 2007 Versus 2017

- Exxon Mobil
- Petrochina
- General Electric
- China Mobile
- ICBC
- Microsoft
- Royal Dutch
- GazProm
- AT&T
- Apple
- Google
- Microsoft
- Facebook
- Coca Cola
- Amazon
- Disney
- Toyota
- McDonalds
- Samsung

DATA IS THE NEW OIL

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
Public school teacher in debt because of identity theft

Published February 26, 2016 10:48pm

A public school teacher may be a victim of identity theft as he owes three banks P800,000 for loans he did not apply for, according to a report by John Consulta on GMA-7’s “24 Oras” on Friday.

Mark Joseph Lontok said he received notifications from three banks saying that he borrowed a total of P800,000 in salary loans. He denied applying for the loans.

However, he remembered posting a photo of his Professional Regulation Commission (PRC) ID online.

“Wala naman akong ginagawang masama,” he added.
55M at risk in ‘Comeleak’

By: Tina G. Santos - Reporter / @santostinaINQ

Philippine Daily Inquirer / 12:44 AM April 23, 2016

DECEPTIVE CALM The Comelec office at Palacio del Gobernador in Intramuros, Manila, after office hours. The Comelec says the hacking of its website will not compromise the integrity of national elections on May 9.

EDWIN BACASMAS
MANILA - The National Privacy Commission has started its investigation into the recent hacking of the Commission on Elections (Comelec) after receiving an *initial report* from the poll body Friday.

Under the Data Privacy Act, the National Privacy Commission has to be notified about the hacking. The body is tasked to monitor government agencies and private organizations handling sensitive data.
<table>
<thead>
<tr>
<th>Identity thieves can:</th>
<th>Impact on victims:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get a Loan</td>
<td>denial of credit/loans</td>
</tr>
<tr>
<td>Open Credit Cards</td>
<td>denial of public service</td>
</tr>
<tr>
<td>Open Utility Accounts</td>
<td>denial of medical care</td>
</tr>
<tr>
<td>Apply for a Refund</td>
<td>harassment by collectors</td>
</tr>
<tr>
<td>Apply for Employment</td>
<td>lawsuits</td>
</tr>
<tr>
<td>Get Medical Care</td>
<td>stress/anxiety</td>
</tr>
<tr>
<td>Commit Crime or Fraud</td>
<td>embarrassment</td>
</tr>
<tr>
<td></td>
<td>time/expenses spent on recovery steps</td>
</tr>
</tbody>
</table>
Impact of a Problematic Data Action on Business

- Loss of reputation
- Loss of market share
- Legal liabilities
1998: Yahoo refuses to buy Google for $1 million.
2002: Yahoo realizes its mistake and tries to buy Google for $3 billion. Google says “Give us $5 billion”, Yahoo says no.
2008: Yahoo refuses to be sold to Microsoft for $40 billion dollars.
2016: Yahoo sold for $4.6 billion to Verizon.
ASHLEY MADISON®
Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select ▼

See Your Matches »

Over 37,565,000 anonymous members!

As seen on: Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

Ashley Madison is the world's leading married dating service for discreet encounters

Trusted Security Award

100% DISCREET SERVICE

SSL Secure Site

Over 39,470,000 anonymous members!
Ashley Madison let off with $1.66m fine over huge hack

Customers receive nothing from settlement with US Federal Trade Commission, which decided owner Ruby Corp was unable to pay full $37.5m penalty

The operator of hacked infidelity website Ashley Madison will pay a sharply discounted $1.66m penalty to settle US investigations into lax data security and deceptive practices.

The remainder of a $17.5m settlement was suspended based on privately held Ruby Corp’s ability to pay.

"I recognize that it was a far lower number frankly than I would have liked," said Federal Trade Commission chairwoman Edith Ramirez. "We want them to feel the pain. We don't want them to profit from unlawful conduct. At the same time we are not going to seek to put a company out of business."

The size of the payment means Ashley Madison's customers will not receive any
ROOT CAUSES OF BREACH

- Malicious or criminal attack: 24%
- System Glitch: 47%
- Human Error: 29%

Report: medical data breach found in 90% of industries

By Carol Ko | 07 Jan 2016

Tag: data breach data privacy healthcare information security Verizon Enterprise

A few years ago, Hong Kong was haunted by a string of data leakage cases involving different public authorities including public hospitals, police, fire services and the...

In fact, on a global basis, the healthcare industry was found to be the worst offender of data breaches, among all the industries that involve the handling to personal

“Verizon 2015 Protected Health Information Data Breach Report”

Of all the 392 million records of patient data breaches disclosed worldwide in between 2004 and 2014, 1,403 breaches occurred within the healthcare industry, according to the PHI Data Breach Report. This was far ahead of the next worst offenders: the public sector with 177 data breaches, and the finance industry, with 113 data breaches.
<table>
<thead>
<tr>
<th>Industry</th>
<th>Frequency</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare</td>
<td>23%</td>
<td>340K</td>
</tr>
<tr>
<td>Financial Services</td>
<td>18%</td>
<td>2K</td>
</tr>
<tr>
<td>Education</td>
<td>16%</td>
<td>1K</td>
</tr>
<tr>
<td>Retail</td>
<td>12%</td>
<td>33K</td>
</tr>
<tr>
<td>Restaurants/Hospitality</td>
<td>9%</td>
<td>2.2M</td>
</tr>
</tbody>
</table>

- Healthcare was more frequent but not as severe.
- Restaurants/Hospitality topped the severity list of number of affected individuals.

23% Healthcare
18% Financial Services
12% Retail
Insiders responsible for 68% of network attacks on healthcare organizations

Written by Jessica Kim Cohen | February 24, 2017 | Print | Email

There were 320 breaches of unsecured protected health information in 2016, representing an increase of 18.5 percent over 2015, according to an IBM X-Force Research report.

Lost or stolen **Laptops**, removable **storage devices**, or **paper records**

Stolen laptop may have contained data of 3,600 Children's Hospital of Los Angeles patients

Written by Erin Dietsche (Twitter | Google+) | January 17, 2017 | Print | Email

Children’s Hospital Los Angeles began notifying 3,600 patients that their information may have been on a laptop that was stolen from a physician’s car, according to the *Los Angeles Times*.

During an Oct. 18 burglary, the laptop was allegedly stolen from a physician’s locked car, according to CBS News. It may have contained the names, addresses, medical record numbers and clinical information of patients. Hospital officials said the laptop was protected with a password, but they’re unsure whether it was properly encrypted.

Hospital spokesman Lorenzo Benet said CHLA "believe[s] that all data may have been erased from the device without any patient data being accessed," according to the *Los Angeles Times*.

How do privacy breaches occur?

Paper records stolen from insecure recycling or garbage bins.

Medical billing records found in pile of debris in New Orleans.

Written by Erin Dietsche (Twitter | Google+) | February 08, 2017 | Print | Email

Beatrice August and her husband weren’t expecting to find patients’ medical billing records in a pile of garbage on their New Orleans property, reports WDSU. But that’s exactly what they discovered.

Ms. August said she doesn’t know who dumped the debris on the property, which has been in her family for years.

"We came out here in November and we saw the first pile back there," she told WDSU. "Then when we came two weeks later, my husband and I came to check, and we saw this. We said, 'Oh my goodness, this is somebody's personal information out here.'"
Databases containing personal information being ‘hacked’ into or otherwise illegally accessed by individuals outside of the agency or organization.

**UPDATED: Hospitals in UK National Health Service knocked offline by massive ransomware attack**

The network was likely taken down by the Wanna Deci, one of the most effective ransomware variants for which there’s currently no decryptor available.

**MultiCare Health System breach affects 1,200 patients**

Tacoma, Wash.-based MultiCare Health System has notified approximately 1,200 current and former patients that their information may have been compromised in a recent privacy incident, according to The News Tribune.

In late November, an unauthorized individual may have accessed an employee’s email account. Although MultiCare secured the account, an investigation proved the account may have contained sensitive patient information, including names, genders, dates of birth, addresses, dates of service, account balances and diagnosis and treatment information. Patients’ Social Security numbers and financial information were not disclosed in the email account.
HOW DO PRIVACY BREACHES OCCUR?

Employees accessing or disclosing personal information **outside the requirements** or authorization of their employment.

Virginia Mason Memorial employees illegally access patient health records

Virginia Mason Memorial Hospital recently discovered 51 hospital employees inappropriately accessed patient health records from around October 2016 to January of this year.

According to an article in the Yakima Herald, employees improperly accessed the health information of 419 emergency room patients over a period of about three months.

READ MORE: SSK Potentially Affected by Virus Encroaching Pediatric Servers

ProMedica employees fired for insider breach of nearly 3,500 patients’ data

ProMedica has terminated three employees for accessing patient records at two hospitals for reasons unrelated to their job responsibilities, reports The Toledo Blade.

In total, seven employees accessed 3,472 patients’ medical records at ProMedica’s Bixby Hospital in Adrian, Mich., and Herrick Hospital in Tecumseh, Mich. The three employees who were terminated had no reason to access the records, and the other four had authority to access the records under certain circumstances. The four with access are receiving “extensive disciplinary actions,” Julie Yaroch, DO, president of Bixby and Herrick hospitals, told The Toledo Blade.

The employees accessed patient names, birth dates, medications and clinical information from acute care services. Dr. Yaroch indicated none of the records were printed, and there is no reason to believe the information was recorded for outside use, according to the report.

Another employee of the Toledo, Ohio-based health system alerted hospital administrators of the breach in April, and ProMedica launched an investigation into the incident. Dr. Yaroch informed The Toledo Blade of the breach on Friday.
Information Security versus Data Privacy
A **Breach** is the unauthorized acquisition, access, use, or disclosure of protected information, which compromises the security or privacy of such information.

**Personal Information**

**PRIVACY**

A **Personal data breach** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
**SECURITY**

**Impact on Data**
- Confidentiality
- Integrity
- Availability

**Governance of the unauthorized**

**PRIVACY**

**Impact on people**
- Collection
- Use
- Storage
- Sharing
- Disposal

**Sensitive Personal Information**

**Governance of the authorized**
Survey Results

Importance of The Rights of A Data Subject, Philippines, Jun 2017

- Important: 85%
- Undecided: 12%
- Not Important: 3%

Net*: +83

*Net figure % Likes to know minus % Does Not like to Know, correctly rounded

*Based on the SWS Survey “FILIPINO PUBLIC OPINION ON DATA PRIVACY AND ATTITUDES AND BEHAVIOUR TOWARDS INTERNET USAGE” June 17-21, 2017 National Survey
Survey Results

Extent of Liking or Not Liking to Know Where The Personal Information They Have Provided During Transaction or Application Will Be Used, Philippines, Jun 2017

5% Likes to Know

94% Does Not Like to Know

Net* +89

Note: No answer/Don’t know/Refused responses are not shown.
*Net figure % Likes to know minus % Does Not like to Know, correctly rounded

*Based on the SWS Survey “FILIPINO PUBLIC OPINION ON DATA PRIVACY AND ATTITUDES AND BEHAVIOUR TOWARDS INTERNET USAGE” June 17-21, 2017 National Survey
### Survey Results

**Trust in Private Institutions Holding Personal Information, Philippines, Jun 2017**

<table>
<thead>
<tr>
<th>Institution</th>
<th>Much Trust</th>
<th>Undecided</th>
<th>Little Trust</th>
<th>Net*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schools 100%</td>
<td>90</td>
<td>5</td>
<td>5</td>
<td>+85</td>
</tr>
<tr>
<td>Hospitals/Clinics 100%</td>
<td>80</td>
<td>11</td>
<td>9</td>
<td>+71</td>
</tr>
<tr>
<td>Banks 100%</td>
<td>64</td>
<td>23</td>
<td>12</td>
<td>+52</td>
</tr>
<tr>
<td>GLOBE 99%</td>
<td>51</td>
<td>30</td>
<td>16</td>
<td>+35</td>
</tr>
<tr>
<td>SMART 99%</td>
<td>51</td>
<td>30</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Credit card companies 98%</td>
<td>44</td>
<td>32</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

*BNote: % Much Trust minus Little Trust, correctly rounded.*

*Based on the SWS Survey “FILIPINO PUBLIC OPINION ON DATA PRIVACY AND ATTITUDES AND BEHAVIOUR TOWARDS INTERNET USAGE” June 17-21, 2017 National Survey*
Which of the following will you share with a stranger?
NATIONAL PRIVACY COMMISSION
The Data Privacy Act ("DPA") of 2012

Data privacy - acknowledging the rights of Data Subjects over their data and enforcing the responsibilities of entities who process them.
The Privacy Ecosystem

You
The Data Subject

Regulators
The NPC

Organizations
Personal Information
Controllers & Processors
Philippine Constitution
Article 3, Bill of Rights

• **Section 2.** Right to be secure in their persons, houses, papers, and effects against unreasonable searches

• **Section 3.** Privacy of communication and correspondence

• **Section 5.** Free exercise and enjoyment of religious profession and worship

• **Section 6.** Liberty of abode and the right to travel

• **Section 8.** Right to information, and access to official records
Philosophy

Risk management approach | Prevention and mitigation | Building the culture of data privacy and protection
Risk Management

- Risk can never be eliminated, so it must be managed.

Risk Responses

- Accept risk
- Avoid risk
- Mitigate risk
- Transfer/share risk
What is a *Privacy Risk*?

A Personal Data Breach and a Data Privacy Violation that has *NOT* happened yet.
AN

introduction

TO THE

Data Privacy Act
STRUCTURE OF RA 10173

Sections 1-6.
Definitions and General Provisions

Sections 7-10.
The National Privacy Commission

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

Sections 22-24.
Provisions Specific to Government

Sections 25-37.
Penalties
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 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 DATA PRIVACY ACT OF 2012
The rights of a Data Subject
An individual whose **personal, sensitive personal or privileged information is processed.**
RIGHTS OF A DATA SUBJECT

Right to Object

Right to Access

Right to be Informed
Right to Block/Remove

Right to Correct/Rectify

Right to Data Portability
Right to File a Complaint

Right to be Indemnified
THE DATA PRIVACY ACT OF 2012

The obligations of data controllers and processors
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;
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.
OBLIGATIONS OF A PERSONAL INFORMATION CONTROLLER

The PIC should collect personal information for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection.

The PIC should process personal information fairly and lawfully, and in accordance with the rights of a data subject.

The PIC should process accurate, relevant and up to date personal information.

The PIC should collect and process personal information adequately and not excessively.

The PIC should retain personal information only for as long as necessary for the fulfillment of the purposes for which the data was obtained. The information should be kept in a form which permits identification of data subjects for no longer than is necessary.

The PIC must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information.
THE DATA PRIVACY ACT OF 2012

The National Privacy Commission
Functions

Advisory
Advocacy
Investigation
Compliance & Monitoring
Public Education
Complaints
Enforcement

Rule-Making
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.
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

CREATE AND COLLECT

STORE AND TRANSMIT

DISPOSE AND DESTROY

USE AND DISTRIBUTE

RETAIN
## I. CREATE AND COLLECT

<table>
<thead>
<tr>
<th>Punishable Act</th>
<th>Imprisonment</th>
<th>Fine (PHP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Purposes</td>
<td>18 months to 5 years — 2 years to 7 years</td>
<td>500 thousand to 2 million</td>
</tr>
<tr>
<td>Unauthorized Processing of Personal Information/Records</td>
<td>1 year to 3 years — 3 years to 6 years</td>
<td>500 thousand to 4 million</td>
</tr>
</tbody>
</table>
## II. STORE AND TRANSMIT

<table>
<thead>
<tr>
<th>Punishable Act</th>
<th>Imprisonment</th>
<th>Fine (PHP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessing of Personal Information and Sensitive Personal Information due to Negligence</td>
<td>1 year to 3 years — 3 years to 6 years</td>
<td>500 thousand to 4 million</td>
</tr>
<tr>
<td>Intentional Breach</td>
<td>1 year to 3 years</td>
<td>500 thousand to 2 million</td>
</tr>
<tr>
<td>Malicious Disclosure</td>
<td>18 months to 5 years</td>
<td>500 thousand to 1 million</td>
</tr>
<tr>
<td>Unauthorized Disclosure</td>
<td>1 year to 3 years — 3 years to 5 years</td>
<td>500 thousand to 2 million</td>
</tr>
</tbody>
</table>
## III. USE AND DISTRIBUTE

<table>
<thead>
<tr>
<th>Punishable Act</th>
<th>Imprisonment</th>
<th>Fine (PHP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Processing of Personal Information and Sensitive Personal Information</td>
<td>1 year to 3 years — 3 years to 6 years</td>
<td>500 thousand to 4 million</td>
</tr>
<tr>
<td>Unauthorized Purposes</td>
<td>18 months to 5 years — 2 years to 7 years</td>
<td>500 thousand to 2 million</td>
</tr>
<tr>
<td>Intentional Breach</td>
<td>1 year to 3 years</td>
<td>500 thousand to 2 million</td>
</tr>
<tr>
<td>Concealing Breach</td>
<td>18 months to 5 years</td>
<td>500 thousand to 1 million</td>
</tr>
<tr>
<td>Malicious Disclosure</td>
<td>18 months to 5 years</td>
<td>500 thousand to 1 million</td>
</tr>
<tr>
<td>Unauthorized Disclosure</td>
<td>1 year to 3 years — 3 years to 5 years</td>
<td>500 thousand to 2 million</td>
</tr>
</tbody>
</table>
### IV. RETAIN

<table>
<thead>
<tr>
<th>Punishable Act</th>
<th>Imprisonment</th>
<th>Fine (PHP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access due to Negligence of Records</td>
<td>1 year to 3 years — 3 years to 6 years</td>
<td>500 thousand to 4 million</td>
</tr>
<tr>
<td>Malicious Disclosure</td>
<td>18 months to 5 years</td>
<td>500 thousand to 1 million</td>
</tr>
<tr>
<td>Unauthorized Disclosure</td>
<td>1 year to 3 years — 3 years to 5 years</td>
<td>500 thousand to 1 million</td>
</tr>
</tbody>
</table>
## V. DISPOSE AND DESTROY

<table>
<thead>
<tr>
<th>Punishable Act</th>
<th>Imprisonment</th>
<th>Fine (PHP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improper Disposal of Records</td>
<td>6 months to 3 years</td>
<td>100 thousand to 1 million</td>
</tr>
<tr>
<td>Access due to Negligence</td>
<td>1 year to 3 years to 6 years</td>
<td>500 thousand to 4 million</td>
</tr>
<tr>
<td>Concealing Breach</td>
<td>18 months to 5 years</td>
<td>500 thousand to 1 million</td>
</tr>
</tbody>
</table>
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.
HOW TRANSPARENCY IS DEMONSTRATED

- CONSENT
- PRIVACY NOTICE
- PRIVACY POLICY
Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.
**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.
**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 Risks: 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 Importance of a Data Protection Officer
The champion of privacy within your organization.

Your point of contact for data subjects and the NPC.
When will you hear from the NPC?

1. When the NPC sends advisories and circulars
2. When the NPC conducts audit and compliance checks
3. When you notify the NPC about a personal data breach
What do we look for when the NPC comes knocking at your door?

1. Can we feel a culture of Privacy?
2. Do you have a sensible data privacy program?
3. Is it based on risk assessment?
4. Do you train your staff in data privacy and protection?
5. Are you prepared for breach?
THE NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK

I. GOVERNANCE
- A. Choose a DPO
- B. Register
- C. Records of processing activities
- D. Conduct PIA

II. RISK ASSESSMENT
- E. Privacy Management Program
- F. Privacy Manual

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

IV. DAY TO DAY
- J. Organizational
- K. Physical
- L. Technical
  - M. Data Center
  - N. Encryption
  - O. Access Control Policy

V. DATA SECURITY
- P. Training and Certifications
- Q. Security Clearances

VI. BREACHES
- T. Data Breach Management
  - U. Security Policy
  - V. Data Breach Response Team
  - W. Incident Response Procedure
  - X. Document
  - Y. Breach Notification

VII. THIRD PARTIES
- Z. Third Parties:
  - A. Legal Basis for Disclosure
  - B. Data Sharing Agreements
  - C. Cross Border Transfer Agreement

VIII. MANAGE HR
- D. V. Trainings and Certifications
- E. W. Security Clearances

IX. CONTINUITY
- F. X. Continuing Assessment and Development
  - G. Regular PIA
  - H. Review Contracts
  - I. Internal Assessments
  - J. Review PMP
  - K. Accreditations

X. PRIVACY ECOSYSTEM
- L. Y. New technologies and standards
- M. Z. New legal requirements
<table>
<thead>
<tr>
<th>I. Establishing Data Privacy Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Appointment of your Data Privacy Officer (DPO)</td>
</tr>
<tr>
<td>2. Register</td>
</tr>
<tr>
<td>3. Records of processing activities</td>
</tr>
<tr>
<td>4. Conduct of a Privacy Impact Assessment (PIA)</td>
</tr>
<tr>
<td>5. Formulate your organization’s privacy management program (PMP)</td>
</tr>
<tr>
<td>6. Craft your agency’s privacy manual</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>II. Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Formulating policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them</td>
</tr>
<tr>
<td>8. Policies for limiting data processing according to its declared, specified and legitimate purpose</td>
</tr>
<tr>
<td>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 owner (Data Subject Access Request)</td>
</tr>
<tr>
<td>10. Policies/procedures that allow data subjects to dispute inaccuracies or errors of their personal information including policies/procedures to keep the same up to date</td>
</tr>
<tr>
<td>11. Policies/procedures that allow data subjects to suspend, withdraw or order the blocking, removal or destruction of their personal information</td>
</tr>
<tr>
<td>12. Policies/procedures for accepting and addressing complaints from data subjects</td>
</tr>
<tr>
<td>13. Policies/procedures that allow data subjects to get indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false and unlawfully obtained or unauthorized use of personal information</td>
</tr>
<tr>
<td>14. Policies/procedures that allow data subjects to obtain a copy of their personal data processed by electronic means and in a structured and commonly used format</td>
</tr>
<tr>
<td>15. Policies/procedures for creation and collection, storage, transmission, use and distribution, retaining personal data for only a limited period or until the purpose of the processing has been achieved, and ensuring that data is securely destroyed or disposed of</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>III. Preparing Your Organization’s Data Privacy Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>16. Policies/procedures for ensuring appropriate and sufficient organizational security measures (policies and procedures in place)</td>
</tr>
<tr>
<td>17. Implement appropriate and sufficient physical security measures (Physical Access and Security, Design and Infrastructure)</td>
</tr>
<tr>
<td>18. Implement appropriate and sufficient technical security measures (Firewalls, Encryption, Access Control Policy, Security for Data Storage, and Other Information Security Tools)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IV. Privacy in Day-to-Day Information Life Cycle Operations (To Be Included in the Privacy Manual)</th>
</tr>
</thead>
<tbody>
<tr>
<td>19. Compliance with the DPA’s Data Breach Management Requirements (e.g. Security Policy, Data Breach Response Team, Incident Response Procedure, Document, Breach Notification)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>V. Managing Personal Data Security Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>20. Managing Third Party Risks</td>
</tr>
<tr>
<td>21. Maintaining data privacy requirements (Legal Basis for Disclosure, Data Sharing Agreements, Cross Border, Security of Transfers) for third parties (e.g. clients, vendors, processors, affiliates)</td>
</tr>
<tr>
<td>22. Periodic and mandatory personal training on privacy and data protection in general and in areas reflecting job-specific content</td>
</tr>
<tr>
<td>23. Issuance of Security Clearances for those handling personal data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VI. Data Breach Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>24. Review of forms, contracts, policies, and processes on a regular basis</td>
</tr>
<tr>
<td>25. Scheduling of Regular Compliance Monitoring, Internal Assessments and Security Audits</td>
</tr>
<tr>
<td>27. Regular evaluation of Privacy Management Program</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VII. Managing Human Resources (HR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>28. Establishing a culture of privacy by obtaining certifications or accreditations visa-vis existing international standards</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VIII. Continuing Assessment and Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>29. Monitoring of emerging technologies, new risks of data processing, and the Privacy Ecosystem</td>
</tr>
<tr>
<td>30. Keeping track of data privacy best practices, sector specific standards, and international data protection standards</td>
</tr>
<tr>
<td>31. Seeking guidance and legal opinion on new National Privacy Commission (NPC) issuances or requirements</td>
</tr>
</tbody>
</table>
Data Privacy Act Checklist

Data Privacy Act (RA 10173) Checklist

<table>
<thead>
<tr>
<th>Signs of Compliance, Commitment to Comply, Capacity to Comply</th>
<th>vs.</th>
<th>Signs of Negligence</th>
</tr>
</thead>
</table>

**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>
The Data Privacy Golden Rule

If you Can’t Protect It

Don’t Collect It.
“Laws too gentle are seldom obeyed; too severe, seldom executed.”  Benjamin Franklin
Ang personal information mo parang pagmamahal lang.

AGE
MARITAL STATUS
ETHNICITY
NATIONALITY
PHILOSOPHICAL AFFILIATIONS
FULL MAIDEN NAME OF MOTHER
EXPENDITURES AND DEBTS
HEALTH
EDUCATIONAL ATTAINMENT
SIBLINGS
FULL ADDRESS
E-MAIL ADDRESS
CONTACT NUMBERS
PIN CODE
PASSWORDS
SOCIAL SECURITY NUMBER
PASSPORT INFORMATION
TAX RETURNS
CURRENT HEALTH RECORDS
GENETIC RECORDS
POLITICAL STANCE
LIKES WATCHING HAMSTER, CORGI, AND HIPHOP MUSIC, VIDEOS
DOWNLOADS ENTIRE SARAH Geronimo Discography
DISLIKES CINNAMON, WEEKDAYS, AND STRICT BOSSES
HAS THREE CHILDREN, TWO BOYS AND ONE GIRL
LIKES POSTING ABOUT #MATCHY Matchy
CONNECTS TO THE INTERNET VIA 2G
WORKS AT EDI SA PUSO MO
VISITED HONG KONG
LIFE REGS
SEARCH

Dapat sa tamang tao napupunta.
...But that’s what we were made to handle. For #DataPrivacy concerns and complaints, e-mail us at complaints@privacy.gov.ph.
Beware, sweetie! Your cellphone is being hacked and you are about to lose your personal information.

Data Protection Tips:

1. Use strong passwords.
2. Keep your software up to date.
3. Be cautious with downloads.

Follow these tips to protect your data.
2017 DATA PROTECTION OFFICERS (DPO) SUMMIT

DPO Assembly For the Government Sector, Landbank of the Philippines, Manila, April 5, 2017 (347 participants)

DPO Assembly For the Banking Industry, BSP Assembly Hall, Bangko Sentral ng Pilipinas, Pasay City, May 31, 2017 (129 participants)

DPO Assembly For Telecommunication Industry, GT-Toyota Asian Center Auditorium, University of the Philippines- Diliman, Quezon City, August 1, 2017 (181 participants)
SITH HAPPENS

...But that’s what we were made to handle.
For #DataPrivacy concerns and complaints,
e-mail us at complaints@privacy.gov.ph.
NPC SECTORAL APPROACH

- Health
- TELCO
- Banks & Non-Bank Financial Institutions
- Education & Research
- Media & Social Media
- BPO
- Retail, Hospitality, Tourism
- Transportation & Logistics
- Real Estate
- Pharmaceutical Industry
- Direct Marketing & Networking
- Workplace
- Utilities
- Government
Building Resiliency. Enforcing the Data Privacy Act
COMPLIANCE
doing what’s required

ACCOUNTABILITY
doing what’s necessary
COMPLIANCE
blind trust
ACCOUNTABILITY
proven trust
PRIVACY.GOV.PH

facebook.com/privacy.gov.ph
twitter.com/privacyph
info@privacy.gov.ph
920-0101 (Local)
7001 OPC
7021 PIAD
7041 CMD