The Data Privacy Act of 2012 Impact and Significance To the Retail Industry

RAYMUND ENRIQUEZ LIBORO
PRIVACY COMMISSIONER AND CHAIRMAN
What the **law** is all about

How it will affect **you**
Information Privacy Then...

Persons, houses, papers, and effects

Correspondence

Communication

protected from government intrusions through illegal searches
What is private then was what was found within the four corners of your **home** and within the confidentiality of communication.
Shift of Perspective

From the **household** to a **reasonable** expectation of privacy

What a person knowingly exposes to the public, even in his own house or office, is not what is private,

**But what he seeks to preserve as private, even in a public area.**
From Industrial Revolution

To Information Revolution
The Information Age

The Info Structure Environment
The Information Age

The Info Structure Environment

The Information Age

Potential Dangers

Internal

External

RA 10173
THE DATA PRIVACY
ACT OF 2012
The Product of a 21st Century Law

For Addressing 21st Century Concerns
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
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**
Technology eliminates the Middleman

DATA as the common Denominator

UBER  FACEBOOK  ALIBABA  AIRBNB
<table>
<thead>
<tr>
<th>2007</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exxon Mobil</td>
<td>Apple</td>
</tr>
<tr>
<td>Petrochina</td>
<td>Google</td>
</tr>
<tr>
<td>General Electric</td>
<td>Microsoft</td>
</tr>
<tr>
<td>China Mobile</td>
<td>Facebook</td>
</tr>
<tr>
<td>ICBC</td>
<td>Coca Cola</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Amazon</td>
</tr>
<tr>
<td>Royal Dutch</td>
<td>Disney</td>
</tr>
<tr>
<td>GazProm</td>
<td>Toyota</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>McDonalds</td>
</tr>
<tr>
<td></td>
<td>Samsung</td>
</tr>
</tbody>
</table>
Impact of a Problematic Data Action on Business

- Loss of reputation
- Loss of market share
- Legal liabilities
ROOT CAUSES OF BREACH

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

88 percent of retailers vulnerable to data breaches in 2017

By Retail Tech Innovation editors | 2017-08-01

The 2017 Thales Data Threat Report, Retail Edition revealed that 43% of retailers had experienced a data breach in the last year with 32% claiming a breach occurring more than once. Produced in conjunction with analyst firm 451 Research also revealed that 88% of retailers consider themselves vulnerable to data threats past year.
Industries Affected

- 23% Healthcare
- 18% Financial Services
- 16% Retail
- 6% Government
- 6% Insurance
- 9% Restaurants/Hospitality
- 2% Professional Services
- 8% Other
Employees accessing or disclosing personal information **outside the requirements or authorization** of their employment.
Target Data Breach Has Cost Banks $240M So Far

February 21, 2014 • min read by Christine DiGangi Comments 0 Comments

The Target data breach has caused a lot of headaches — it has also been crazy expensive.

A new report from the Consumer Bankers Association estimates the cost of replacing the credit and debit cards compromised in the breach has exceeded $200 million. That’s just card-replacement costs reported by the CBA and the Credit Union National Association. Factor in the impact of fraudulent activity and costs to financial institutions not members of the CBA or CUNA, and the price tag on the Target data breach gets a lot higher.

Databases containing personal information being ‘hacked’ into or otherwise illegally accessed by individuals outside of the agency or organization

Home Depot breach totals: 56 million credit cards exposed, $62 million in losses

19 SEP 2014 10
Cryptography, Data loss, Law & order, Malware
Databases containing personal information being ‘hacked’ into or otherwise illegally accessed by individuals outside of the agency or organization.
DATA PRIVACY RELATED DIFFICULTIES

- Customer database breaches
- Company’s lack of adequate policies to protect customer information
- Payment card security breaches
- Customer profiling leading to transparency concerns
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
Survey Results

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

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

Net* +83

85%
12%
3%

Important  Undecided  Not Important

*Net figure % Likes to know minus % Does Not like to Know, correctly rounded
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, June 2017

94% Likes to Know
5% Does Not Like to Know

Net* +89

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

Note: No answer/Don’t know/Refused responses are not shown.
*Net figure % Likes to know minus % Does Not like to Know, correctly rounded
Nature of Complaints (as of August 31, 2017)

<table>
<thead>
<tr>
<th>Classification</th>
<th>No. of Complaints</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Processing</td>
<td>40</td>
<td>28%</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Unauthorized Access/Intentional Breach</td>
<td>7</td>
<td>5%</td>
</tr>
<tr>
<td>Unauthorized Disclosure</td>
<td>6</td>
<td>4%</td>
</tr>
<tr>
<td>Rights of Data Subject</td>
<td>13</td>
<td>9%</td>
</tr>
<tr>
<td>Security of Personal Information</td>
<td>32</td>
<td>22%</td>
</tr>
<tr>
<td>General Inquiry</td>
<td>20</td>
<td>14%</td>
</tr>
<tr>
<td>Others - CID</td>
<td>5</td>
<td>3%</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>16</td>
<td>11%</td>
</tr>
<tr>
<td>Theft</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Consumer Protection</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Credit Card</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Drone</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Total</td>
<td>145</td>
<td>100%</td>
</tr>
</tbody>
</table>
RA 7610 Special Protection of Children against Abuse Act

RA 8484 Access Devices Regulation Act

RA 8792 Electronic Commerce Act

RA 9208 Anti-Trafficking Act

RA 9262 Anti-Violence against Women and Children Act

RA 9775 Anti-Child Pornography Act

RA 9995 Anti-Photo and Video Voyeurism

RA 10173 Data Privacy Act

RA 10175 Cybercrime Prevention 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

introduction

TO THE

Data Privacy Act

OF 2012
FULL TITLE

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 SCOPE AND POLICY OF
THE DATA PRIVACY ACT OF 2012
The Privacy Ecosystem

YOU
The Data Subject

REGULATORS
The NPC

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

- **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.
• PERSONAL INFORMATION CONTROLLERS (PIC) and PERSONAL INFORMATION PROCESSORS (PIP) PROCESSING PERSONAL DATA of DATA SUBJECTS
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.
## 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 2 years — 1 year 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 — 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>
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.
Data Privacy Principles

Security Measures

Uphold Rights of Data Subject
An individual whose **personal, sensitive personal or privileged information** is processed.
RIGHTS OF A DATA SUBJECT

Right to be Informed

Right to Object

Right to Access
RIGHTS OF A DATA SUBJECT

- Right to Correct/Rectify
- Right to Block/Remove
- Right to Data Portability
RIGHTS OF A DATA SUBJECT

Right to File a Complaint

Right to be Indemnified
KEY CONCEPTS
**CLASSIFICATION OF PERSONAL DATA**

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

Refers to personal information about an individual’s:

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

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

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

and specifically established by an executive order or an act of Congress to be kept classified.
<table>
<thead>
<tr>
<th>Personal Information</th>
<th>Sensitive Personal Information (List based on IRR)</th>
<th>Privileged Information (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>Data received within the context of a protected relationship – attorney and client</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>Data received within the context of a protected relationship – priest and penitent</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>
Which data is personal information?

- A) November 30, 1863
- B) Filipino, male, born on November 30, 1863
- C) Philippine Hero, born on November 30, 1863
PERSONAL INFORMATION CONTROLLER

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

It excludes:

- A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or

- A natural person who processes personal data in connection with his or her personal, family, or household affairs;
PERSONAL INFORMATION PROCESSOR

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

NOTICE
TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY
TRANSPARENCY

Principle of Transparency
A data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
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.
If It’s NOT CLEAR

It’s NOT Consent
Sometimes, consent is NOT necessary...

- Personal Information (not Sensitive)
- Contractual or Legal Obligation
- National Emergency, public order, public safety
- Legitimate interests
- To protect life, health, vitally important interests
Sometimes, consent is NOT necessary...

To protect life and health

Sensitive Personal Information

Protection of rights in court

Provided to government under legal mandate

Law/Regulation

SUBPOENA
**Principle of Legitimate Purpose**

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

---

**Principle of Proportionality**

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

Pillars of Compliance
1. Commit to Comply: Appoint a **Data Protection Officer** (DPO).

2. Know Your Risks: Conduct a **Privacy Impact Assessment** (PIA).

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

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

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
   P. Data Life Cycle

IV. DAY TO DAY
   Q. Organizational
   R. Physical
   S. Technical
      ▶ Data Center
      ▶ Encryption
      ▶ Access Control Policy

V. DATA SECURITY
   T. Data Breach Management;
      ▶ Security Policy
      ▶ Data Breach Response Team
      ▶ Incident Response Procedure
      ▶ Document
      ▶ Breach Notification

VI. BREACHES
   U. Third Parties;
      ▶ Legal Basis for Disclosure
      ▶ Data Sharing Agreements
      ▶ Cross Border Transfer Agreement

VII. THIRD PARTIES

VIII. MANAGE HR
   V. Trainings and Certifications
   W. Security Clearance

IX. CONTINUITY
   X. Continuing Assessment and Development
      ▶ Regular PIA
      ▶ Review Contracts
      ▶ Internal Assessments
      ▶ Review PMP
      ▶ Accreditations

X. PRIVACY ECOSYSTEM
   Y. New technologies and standards
   Z. New legal requirements
**I. Establishing Data Privacy Governance**

1. Appointment of your Data Privacy Officer (DPO)

2. Register

3. Records of processing activities

4. Conduct of a Privacy Impact Assessment (PIA)

**II. Risk Assessment**

5. Formulate your organization's privacy management program (PMP)

6. Craft your agency's privacy manual

**III. Preparing Your Organization's Data Privacy Rules**

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

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

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

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

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

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

13. Policies/procedures for accepting and addressing complaints from data subjects

14. 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.

15. Policies/procedures that allow data subjects to obtain from the personal information controller a copy of his or her personal data processed by electronic means and in a structured and commonly used format

16. 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

**IV. Privacy in Day-to-Day Information Life Cycle Operations (To Be Included in the Privacy Manual)**

17. Implement appropriate and sufficient organizational security measures (Policies and procedures in place)

18. Implement appropriate and sufficient physical security measures (Physical Access and Security, Design and Infrastructure)

19. Implement appropriate and sufficient technical security measures (Firewalls, Encryption, Access Control Policy, Security of Data Storage, and Other Information Security Tools)

**V. Managing Personal Data Security Risks**

20. Compliance with the DPA's Data Breach Management Requirements (e.g. Security Policy, Data Breach Response Team, Incident Response Procedure, Document, Breach Notification)

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)

22. Managing Human Resources (HR)

23. Issuance of Security Clearance for those handling personal data

24. Scheduling of Regular PIA for new and existing programs, systems, processes and projects

25. Review of Forms, Contracts, Policies and Procedures on a regular basis

26. Scheduling of Regular Compliance Monitoring, Internal Assessments and Security Audits

27. Review, validation and update of Privacy Manual

28. Regular evaluation of Privacy Management Program

29. Establishing a culture of privacy by obtaining certifications or accreditations vis-à-vis existing international standards

**VI. Data Breach Management**

30. Monitoring of emerging technologies, new risks of data processing, and the Privacy Ecosystem

31. Keeping track of data privacy best practices, sector specific standards, and international data protection standards

32. Seeking guidance and legal opinions on new National Privacy Commission (NPC) issuances or requirements
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**?
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
The Data Privacy Golden Rule

If you Can’t Protect It... DON'T Collect It.