Security Measures & Registration of Data Processing Systems

Dr. Rolando R. Lansigan
Chief, Compliance and Monitoring Division
SECURITY MEASURES
1. Technical

2. Organisational – other measures
<table>
<thead>
<tr>
<th>Encryption</th>
<th>Backups</th>
</tr>
</thead>
<tbody>
<tr>
<td>To what standard? (cost Vs benefit)</td>
<td>Secure: encrypted tapes / cloud-provider</td>
</tr>
<tr>
<td>All devices or just some?</td>
<td>Auditable process</td>
</tr>
<tr>
<td>Passwords</td>
<td>Access control</td>
</tr>
<tr>
<td>Enforced strength and updates?</td>
<td>Who decides permissions and privileges ('need to know')?</td>
</tr>
<tr>
<td>Sharing data</td>
<td>Remote access</td>
</tr>
<tr>
<td>Technical solutions – e.g. via email; portals</td>
<td>How delivered securely?</td>
</tr>
<tr>
<td>System testing &amp; maintenance</td>
<td>Permit Bring Your Own Device?</td>
</tr>
<tr>
<td>Who has access, to what (System Administrators)</td>
<td></td>
</tr>
<tr>
<td>Live or dummy data?</td>
<td></td>
</tr>
<tr>
<td>Firewalls / Anti-virus / Spam filters</td>
<td></td>
</tr>
</tbody>
</table>
Organisational – physical security

Secure Office Storage

For removable devices and hardcopy information

- Identifying marks?
- Kensington locks?

Remote working

- Secure both hardcopies and devices when in transit.

Remote working

Kept out of sight: in transit | at home.

Secure disposal

- Lockable pedestals | Kensington locks?

Secure disposal

- Shredding of hardcopies
- Beyond use | Reuse | Resale

Building access control

Secure premises – CCTV | locked windows | perimeter

- Locked CCTV room | server room

- ID badges, supervised visitors | contractors
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
- Disciplinary process
- Training records

Procurement (and contracts)

- i.e. outsourced services like IT and software
- Due diligence
- Auditing and monitoring
- Compliant contract Terms and Conditions:
  - Act on your instructions
  - Equivalent security
REGISTRATION OF DATA PROCESSING SYSTEMS
Timeline of DPA Law and IRRs passed to Organization’s Compliance

- **2012**
  - Data Privacy Act (DPA) Passed into law

- **March 2016**
  - National Privacy Commission (NPC) was formed

- **August 2016**
  - Implementing rules and Regulations (IRRs) was published

- **Sept. 9, 2016**
  - IRRs came into effect (comply with all provisions except registration requirements)

- **Sept. 9, 2017**
  - Comply with registration requirements

**Registration Requirements:** All personal data processing systems (DPS) operating in the Philippines that (1) employs at least 250 employee; OR (2) processes at least 1,000 sensitive personal information; OR (3) data processing is likely to pose a risk to the rights and freedoms of data subjects; or (4) service providers to government must be registered with NPC

12 months
Register with the NPC (Legal Basis: Sec. 24, IRR 33 and 46-49)

<table>
<thead>
<tr>
<th>COMPLIANT</th>
<th>NON-COMPLIANT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register with the NPC</td>
<td>Non-registration with the NPC</td>
</tr>
<tr>
<td>- Registration with the NPC is up-to-date and contains all necessary</td>
<td>- No registration (must be renewed annually)</td>
</tr>
<tr>
<td>compliance documentation</td>
<td>- Out-of-date registration (must be updated within three months of any</td>
</tr>
<tr>
<td>- Registration of all automated processing operations that have legal</td>
<td>change)</td>
</tr>
<tr>
<td>effect on the data subject</td>
<td>- Non-reporting to NPC of documented security incidents and personal data</td>
</tr>
<tr>
<td>- Annual report summarizing documented security incidents and personal</td>
<td>breaches</td>
</tr>
<tr>
<td>data breaches</td>
<td></td>
</tr>
<tr>
<td>- Service providers are also registered</td>
<td></td>
</tr>
</tbody>
</table>
Who should register?

Personal Information Controllers and Personal Information Processors who:

- employ more than 250 persons
- process sensitive personal information of at least 1,000 individuals
- belong to sectors identified by the NPC where:
  - the processing carried out is likely to pose a risk to the rights and freedoms of data subjects, and
  - the processing is not occasional
- are service providers to government.
Section 47. Registration of Personal Data Processing Systems.

The personal information controller or personal information processor that employs fewer than two hundred fifty (250) persons shall not be required to register unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal information of at least one thousand (1,000) individuals.
a. The contents of registration shall include:

1. The name and address of the personal information controller or personal information processor, and of its representative, if any, including their contact details;
2. The purpose or purposes of the processing, and whether processing is being done under an outsourcing or subcontracting agreement;
3. A description of the category or categories of data subjects, and of the data or categories of data relating to them;
4. The recipients or categories of recipients to whom the data might be disclosed;
5. Proposed transfers of personal data outside the Philippines;
6. A general description of privacy and security measures for data protection;
7. Brief description of the data processing system;
8. Copy of all policies relating to data governance, data privacy, and information security;
9. Attestation to all certifications attained that are related to information and communications processing; and
10. Name and contact details of the compliance or data protection officer, which shall immediately be updated in case of changes.

b. The procedure for registration shall be in accordance with these Rules and other issuances of the Commission.
Phases of Registration

Phase ONE –

Phase TWO -
### PERSONAL INFORMATION CONTROLLER

<table>
<thead>
<tr>
<th>NAME OF THE ORGANIZATION</th>
<th>EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPANY ADDRESS</td>
<td>TEL. NO.</td>
</tr>
</tbody>
</table>

### HEAD OF THE ORGANIZATION

<table>
<thead>
<tr>
<th>LAST NAME</th>
<th>EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIRST NAME</td>
<td>TEL. NO.</td>
</tr>
<tr>
<td>MIDDLE INITIAL</td>
<td></td>
</tr>
</tbody>
</table>

### OFFICIAL DESIGNATION (CEO/President)

### DATA PROTECTION OFFICER

<table>
<thead>
<tr>
<th>LAST NAME</th>
<th>EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIRST NAME</td>
<td>TEL. NO.</td>
</tr>
<tr>
<td>MIDDLE INITIAL</td>
<td>MOBILE NO.</td>
</tr>
</tbody>
</table>

### OFFICIAL DESIGNATION: STATUS (PERMANENT: YES)

### SWORN STATEMENT

I declare under oath that this Registration Form is accomplished by Data Protection Officer, and is a true 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 validate the contents stated herein.

__________________________  ____________________________
Head of Agency               Data Protection Officer
(Signature over Printed Name) (Signature over Printed Name)

SUBSCRIBED and SWORN to before me, the undersigned Notary Public, who exhibited to me (either) Government issued ID No. ____________

__________________________
Notary Public

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

<table>
<thead>
<tr>
<th>NFC ACCESS CODE</th>
<th>APPROVED BY [SIGNATURE OVER PRINTED NAME]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DATE GIVEN [MM/DD/YYYY]</td>
</tr>
</tbody>
</table>
### Personal Information Controller

<table>
<thead>
<tr>
<th>NAME OF THE ORGANIZATION</th>
<th>EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEBSITE (URL)</td>
<td></td>
</tr>
<tr>
<td>COMPANY ADDRESS</td>
<td>TEL. NO.</td>
</tr>
</tbody>
</table>

### Head of the Organization

<table>
<thead>
<tr>
<th>LAST NAME</th>
<th>EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIRST NAME</td>
<td>TEL. NO.</td>
</tr>
<tr>
<td>MIDDLE INITIAL</td>
<td></td>
</tr>
</tbody>
</table>

### Official Designation (CEO/President)

<table>
<thead>
<tr>
<th>POSITION</th>
</tr>
</thead>
</table>

### Data Protection Officer

<table>
<thead>
<tr>
<th>LAST NAME</th>
<th>EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIRST NAME</td>
<td>TEL. NO.</td>
</tr>
<tr>
<td>MIDDLE INITIAL</td>
<td>MOBILE NO.</td>
</tr>
<tr>
<td>OFFICIAL DESIGNATION</td>
<td>STATUS (PERMANENT: Y/N)</td>
</tr>
</tbody>
</table>
Phase 2 - Registration

Process Owner
Name of Data Processing System
Purpose of Processing
Processing as PIP, PIC or both
Outsourced or Sub Contracted
Description of the Category
Recipients or Categories of Recipients to whom the personal data might be disclosed
Personal data is transferred outside of the Philippines?
“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