SOME Key Concepts

Hint: It's not all about I.T.
Key concepts

**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.

– RA. 10173, Section 3.g
Key concepts

*Sensitive personal information* refers to personal information:

1. About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

2. About an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

3. 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

4. Specifically established by an executive order or an act of Congress to be kept classified.

– RA. 10173, Section 3.1
<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></td>
</tr>
<tr>
<td>Location of an individual at a particular time</td>
<td>Religious affiliation</td>
<td>Data received within the context of a protected relationship – attorney and client</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>Data received within the context of a protected relationship – priest and penitent</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>
</tbody>
</table>
| **Sensitive Personal Information**  
| (List based on IRR) |
|----------------------|------------------|
| Social security number |
| Licenses or its denials, suspension or revocation |
| Tax returns |
| Other personal info issued by government agencies |
| Bank and credit/debit card numbers |
| Websites visited |
| Materials downloaded |
| Any other information reflecting preferences and behaviors of an individual |
| Grievance information |
| Discipline information |
| Leave of absence reason |
| Licenses or its denials, suspension or revocation |
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.
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
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 Obligations which must be complied with by Government

<table>
<thead>
<tr>
<th>2016 Series (issued)</th>
<th>2017 Series (planned)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circular 1</td>
<td>Circular</td>
</tr>
<tr>
<td>Gov’t Agencies</td>
<td>BSP-Supervised</td>
</tr>
<tr>
<td>Circular 2</td>
<td>Circular</td>
</tr>
<tr>
<td>Data Sharing</td>
<td>DOH-Regulated</td>
</tr>
<tr>
<td>Circular 3</td>
<td>Circular</td>
</tr>
<tr>
<td>Breach Mgmt</td>
<td>Outsourcing Cos.</td>
</tr>
<tr>
<td>Circular 4</td>
<td></td>
</tr>
<tr>
<td>Rules Procedure</td>
<td></td>
</tr>
</tbody>
</table>

Data Privacy Act of 2012

IRRs (promulgated 2016)
SECTION 36. Transitory Period. Government agencies shall be given a period of one (1) year transitory period from the effectivity of these Rules to comply with the requirements provided herein.

February 1, 2018
Why should you comply?

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

- Sec. 34. Extent of Liability. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or **by their gross negligence, allowed the commission of the crime.**
## I. CREATE AND COLLECT

### Punishable Act

<table>
<thead>
<tr>
<th>Unauthorized Purposes</th>
<th>Unauthorized Processing of Personal Information/Records</th>
</tr>
</thead>
</table>

### Imprisonment

<table>
<thead>
<tr>
<th>Unlawful 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</td>
<td>1 year to 3 years — 3 years to 6 years</td>
<td>500 thousand to 4 million</td>
</tr>
<tr>
<td>Records</td>
<td></td>
<td></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

### The Data Life Cycle

<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>

*Images and logos are not included in the text.*
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 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>
The Data Privacy Act of 2012
Privacy Resilience
with Local Government Units
RESILIENCE AND THE FILIPINO SPIRIT
RESILIENCE AND THE FILIPINO SPIRIT
RESILIENCE AND THE FILIPINO SPIRIT
Resilience

- Resilience
- \textit{rɪ'zɪliəns/}
- \textit{noun}
- 1. the capacity to recover quickly from \textit{difficulties}; toughness.
  - adapt well to change
  - keep going in the face of adversity
**CYBER ATTACKS (REAL-TIME) 2017**

### Norse – Superior Attack Intelligence

Norse maintains the world’s largest dedicated threat intelligence network. With over eight million sensors that emulate over six thousand applications – from Apple laptops, to ATM machines, to critical infrastructure systems, to closed-circuit TV cameras - the Norse Intelligence Network gathers data on who the attackers are and what they’re after. Norse delivers that data through the Norse Appliance, which pre-emptively blocks attacks and improves your overall security ROI, and the Norse Intelligence Service, which provides professional continuous threat monitoring for large networks.

#### LIVE ATTACKS

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Attacker IP</th>
<th>Attacker Geo</th>
<th>Target Geo</th>
<th>Attack Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:56:21.284</td>
<td>185.35.62.250</td>
<td>Geneve, CH</td>
<td>Dubai, AE</td>
<td>smtp</td>
<td>123</td>
</tr>
<tr>
<td>14:56:20.770</td>
<td>122.3.47.120</td>
<td>Parañaque, PH</td>
<td>Lynnwood, US</td>
<td>telnet</td>
<td>23</td>
</tr>
<tr>
<td>15:05:41.557</td>
<td>122.54.132.220</td>
<td>Makati, PH</td>
<td>Dubai, AE</td>
<td>telnet</td>
<td>23</td>
</tr>
<tr>
<td>15:04:19.784</td>
<td>207.46.100.250</td>
<td>Redmond, US</td>
<td>DeKalb Junction, US</td>
<td>smtp</td>
<td>25</td>
</tr>
<tr>
<td>15:04:02.333</td>
<td>122.3.47.120</td>
<td>Parañaque, PH</td>
<td>Lynnwood, US</td>
<td>telnet</td>
<td>23</td>
</tr>
</tbody>
</table>
Privacy Risk Formula

Privacy Risk = **Probability** of a Problematic Data Action * **Impact** of a Problematic Data Action

- **Probability** is a contextual analysis that a data action is likely to create a problem for a representative set of individuals.
- **Impact** is an analysis of the costs should the problem occur.
What is a Privacy Risk?

A Personal Data Breach or a Data Privacy Violation that has NOT happened yet.
What is Privacy Resilience?

A Personal Data Breach or a Data Privacy Violation that was prevented.

A breach and privacy disaster that did not happen.
Disaster
Resilience
A **Breach** is the unauthorized acquisition, access, use, or disclosure of protected information, which compromises the security or privacy of such information.

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.
ROOT CAUSES OF BREACH

- Malicious or criminal attack: 47%
- System Glitch: 29%
- Human Error: 24%
The NPC’s 5 Pillars of Accountability

1. Commit to Comply: APPOINT A DATA PROTECTION OFFICER
2. Know Your Risks: CONDUCT A PRIVACY RISK OR IMPACT ASSESSMENT
3. Write Your Plan: CREATE A PRIVACY MANAGEMENT PROGRAM
4. Be Accountable: IMPLEMENT YOUR PRIVACY AND DATA PROTECTION MEASURES
5. Be Prepared for Breach: REGULARLY EXERCISE YOUR BREACH REPORTING PROCEDURE
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

VI. BREACHES
T. Data Breach Management:
   ▶ Security Policy
   ▶ Data Breach Response Team
   ▶ Incident Response Procedure
   ▶ Document
   ▶ Breach Notification

VII. THIRD PARTIES
U. Third Parties:
   ▶ Legal Basis for Disclosure
   ▶ Data Sharing Agreements
   ▶ Cross Border Transfer Agreement

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
   ▶ A+ certifications

X. PRIVACY ECOSYSTEM
Y. New technologies and standards
Z. New legal requirements
DEVELOPING A PRIVACY MANAGEMENT PROGRAM
Why create a **Privacy Management Program**?

- **Easier to Explain to Staff and Management:** results & benefits
- **Compliance becomes more manageable:** outline of how
- **Save on avoidable ‘clean-up’ expenses:** stronger safeguards
Key Components of a Privacy Management Program

- Organizational Commitment
- Program Controls
- Continue Development
- Governance Structure
- Ensure Implementation
- Review and Revise Programs
Organizational Commitment

Organizations (both public and private) should develop and implement a PMP that give effect to the data privacy principles of the Data Privacy Act of 2012 (RA 10173), specifically Sec 11, Chapter III. This means creating a governance structure, or at the minimum, processes to follow and the mechanism to ensure that they are being followed.
1.1 BUY-IN FROM THE TOP

Top management support is key to a successful PMP and essential for the emergence of a culture of privacy in the organization.

When top management is committed to ensuring that the organization is accountable, the program will have a better chance of success, and a privacy respectful culture will more likely be established.

This means that top management should:

- Appoint the Data Protection Officer(s);
- Endorse a set of program controls; and
- Report to the Board, as appropriate, on the program.
1.2 THE DATA PROTECTION OFFICER

A Data Protection Officer should be appointed or designated to manage the privacy management program. The Data Protection Officer shall be responsible for structuring, designing and managing the privacy management program, including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up.

Specifically, the Data Protection Officer shall:

- establish and implement program controls;
- coordinate with those who are responsible for related disciplines and functions within the organization;
- continuously assess and revise program;
- represent the organization in the event of an inspection or an investigation by the National Privacy Commission; and
- advocate personal data protection within the organization itself.
1.3 REPORTING

The organization/agency should establish internal reporting mechanisms to ensure that the privacy management program is structured and whether it is functioning as expected. In larger organizations, the audience for this information is likely to be top management, and in turn, top management reports to the board of directors. All reporting mechanisms should be reflected in the organization's/agency's program controls.

An effective reporting program has the following characteristics:

- Clearly defines its reporting structure (in terms of reporting on its overall compliance activities) as well as employee reporting structures in the event of a complaint or a potential breach;
- Tests and reports on the results of its internal reporting;
- Documents all of its reporting structure.
Key Components of a **Privacy Management Program**

**Program Controls**

These help ensure that what is mandated in the governance structure is implemented in the organization/agency. Developing these controls will assist the Data Protection Officer in structuring an appropriate privacy management program within the organization/agency. Controls also demonstrate how the organization/agency is compliant with the Data Privacy Act.
2.1 PERSONAL DATA INVENTORY

An organization/agency should know what kinds of personal data it holds, how the personal data is being used, and whether the organization/agency really needs it at all.

Understanding and documenting the types of personal data that an organization collects and where it is held (e.g. whether or not whether the data has been passed to any data controller) are important. This will affect the type of consent the organization/agency obtains from individuals and how the data is protected; and it will make it easier to assist individuals in exercising their data access and correction rights. Every component of an accountable, effective PMP begins with personal data inventory.

Every organization/agency should document:

- the kinds of personal data it holds and where it is held (i.e. within the organization or by the data controller(s)); and
- the reason(s) why it is collecting, using, or disclosing personal data.
2.2 POLICIES

Organizations/agencies should develop and document internal policies that address obligations under the law. These policies should be made available to all employees and updated periodically.

Organizations/agencies should develop internal policies that give effect to the data protection principles in the law. These policies should be documented and should show how they connect to the legal requirements.
Program Controls

Collection of personal data;

Security of personal data;

Accuracy and retention of personal data;

Transparency of organizations/agencies’ personal data policies and practices; and

Use of personal data including the requirements for consent;

Access to and correction of personal data.
2.3 RISK ASSESSMENT TOOLS

Proper use of risk assessment tools can help prevent problems. Fixing a personal data problem after the fact can be costly. Therefore it is vital that careful consideration of the purposes for a particular initiative, product or service, and an assessment that minimizes any personal data impacts is done.
2.4 CAPACITY BUILDING

In order for the PMP to be effective, relevant employees should be made aware of personal data protection generally and to be conversant with the organizations/agencies’ policies and practices for compliance with the law. Those who handle personal data directly may need additional training specifically tailored to their roles. Training and education need to be current.
For personal data protection training and education to be effective, it should:

- Be given to new employees and periodically thereafter;
- Cover the policies and procedures established by the organization;
- Be delivered in an appropriate and effective manner, based on organizational needs; and
- Circulate essential information to relevant employees as soon as practical if an urgent need arises.
2.5 BREACH HANDLING

Personal data breaches are expensive and could lead to loss of trust.

Organizations/agencies should have a procedure in place and an officer or a designated team responsible for managing a personal data breach. Responsibilities for internal and external reporting of the breach should be clear.

In handling personal data breach, organizations/agencies should consider the circumstances of the breach, and decide whether any of the following persons should be notified as soon as practicable:

- The affected data subjects
- The law enforcement agencies;
- The National Privacy Commission;
- Any relevant regulators;
Program Controls

2.7 COMMUNICATION

Organizations/agencies should take all practical steps to ensure employees and customers/citizens can ascertain their personal data policies and practices.

Communication should be clear and easily understandable and not simply a reiteration of the Data Privacy Act. In general, it should:

- Provide enough information so that the public knows the purpose of the collection, use and disclosure of personal data and how long it is retained;
- Include information on who to contact with questions or concerns;
- Be made easily available to individuals.
Key Components of a Privacy Management Program

Continue Development

CONTINUING ASSESSMENT AND DEVELOPMENT

In order to properly protect personal data and meet legal obligations, organizations/agencies should monitor, assess and revise their privacy management framework to ensure it remains relevant and effective.
1. DEVELOP AN OVERSIGHT AND REVIEW PLAN

An oversight and review plan will help the organization keep its PMP on track and up-to-date.

The Data Protection Officer should develop an oversight and review plan on a periodic basis that sets out how and when the PMP's effectiveness will be monitored and assessed. Depending on the organization/agency's compliance and control infrastructure, such plan may be covered in its overall oversight and review system.

The oversight and review plan should establish performance measures and include a schedule of when the policies and other program controls will be reviewed.
II. ASSESS AND REVISE PROGRAM CONTROLS

The effectiveness of program controls should be monitored, periodically audited, and where necessary, revised.
Monitoring, an ongoing process, should address the following questions:

- What are the latest threats and risks?
- Are the program controls addressing new threats and reflecting the latest complaint or audit findings, or guidance of the National Privacy Commission?
- Are new services being offered that involve increased collection, use or disclosure of personal data?
- Is training necessary? If yes, is it taking place? Is it effective? Are policies and procedures being followed? And, is the training program up to date?
Way forward: Compliance of LGUs to the DPA

• Appointment of a DPOs / COPs
  • Capacity Building
    • DPO Workshop Liga ng mga Barangay – Davao City Chapter
• Know your risks (Privacy Impact Assessment)
  • Inventory of data and assess data process flows
• Develop your Privacy management plan based on the risks assessed
  • Issuance of Ordinances related to the DPA
• Implement and communicate your Data Privacy Plan
• Prepare for a breach