DPA, DPO and Government

Ivy D. Patdu, MD, JD
Deputy Privacy Commissioner
National Privacy Commission
Right to Privacy
Which of the Following will you be willing to share with someone you just met?

- Home Address
- Diary
- Credit Card Billing Statement
- Browsing History
- Phone Messages
- Facebook Password
- Password
WHO IS WATCHING YOU?
What can you “buy” with your personal data?
Sign Up
It’s free and always will be.
Be part of a market research study and earn up to ₱3000 a week. Sign up → bit.ly/1nZDEzr
90% of the world’s data have been generated only in the last few years.

SINTEF, Big Data, for better or worse: 90% of world's data generated over last two years (May 22, 2013) available at https://www.sciencedaily.com/releases/2013/05/130522085217.htm (last accessed Dec. 27, 2016).
“In this digital era, information is the currency of power – valuable, coveted, but at a very high risk.”

-Senator Edgardo Angara, sponsorship speech for the Data Privacy Act
RIGHT TO INFORMATION PRIVACY

The individual’s ability to control the flow of information concerning or describing him, which however must be overbalanced by legitimate public concerns. To deprive an individual of his power to control or determine whom to share information of his personal details would deny him of his right to his own personhood.

Data Privacy Act

It is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth.
Data Privacy Act applies to the processing of personal data by any natural and juridical person in the government or private sector.
Which are personal data?

A. “Man born on June 19, 1861”
B. “Philippine national hero born on June 19, 1861”
C. “Jose Protacio Rizal”

D. [Image of Jose Rizal]

Jose Rizal, available at https://en.wikipedia.org/wiki/Jos%C3%A9_Rizal
DATA PRIVACY ACT

- Uphold Rights of Data Subject
- Data Privacy Principles
- Security Measures

DATA PRIVACY ACT
DATA PRIVACY PRINCIPLES
TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY
Rights of Data Subjects

1. Right to Information
2. Right to Object
3. Right to Access
4. Right to Correct
5. Right to Erase
6. Right to Damages
7. Right to Data Portability
8. Right to File a Complaint
CONSENT 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.

The consent shall be evidenced by written, electronic or recorded means.
Sometimes, Consent is NOT necessary.
So, you want to buy a dog? Fill in the form please.

Application to Buy a Dog
• Name:_____________
• Birthday:___________
• Address:___________
• TIN No.:____________
• SSS No.:___________
• PRC ID No.:__________
• No. of Cars owned:___
• Father’s name:_______
• Mother’s maiden name: __________
Para Makautang..
(Please Bring this Requirements)

- 6pcs 2x2 Picture
- 4pcs 1x1 Picture (Whole Body)
- 3 Valid ID's
- Brgy. Clearance
- NBI Clearance
- Mayor's Permit
- Medical
- Cedula
- Birth Certificate (NSO)
- SSS/TIN
- Co-maker
- X-ray (Whole Body)
- Police Clearance
- Proof of Billing
- Form 137
SECURITY MEASURES
SECURITY MEASURES

Organizational
Physical
Technical

Confidentiality
Integrity
Availability
ORGANIZATIONAL SECURITY MEASURES
Data Protection Officer

- Expertise in relevant privacy or data protection policies and practices
- Understanding of the processing operations being carried out by the PIC or PIP
- Knowledge of Sector

THE DPO SHOULD POSSESS SPECIALIZED KNOWLEDGE AND DEMONSTRATE RELIABILITY NECESSARY FOR THE PERFORMANCE OF HIS OR HER DUTIES AND RESPONSIBILITIES.

GDPR will require 75,000 DPOs worldwide, study shows

Privacy Impact Assessment

• Personal Data Flow
  • Source and Collection
  • Accountable and responsible persons
  • Purpose of processing
  • Personal Data Processing
  • Security measures
  • Transfer outside country

• Identify and Assess Privacy Risks
  • Privacy Risk Identification
  • Privacy Risk Analysis
  • Privacy Risk Evaluation (Level of Impact and Likelihood of Risks)

• Address risks
CREATE YOUR DATA PRIVACY MANUAL

• Records of Processing Activities
  ◆ (1) Purpose of processing
  ◆ (2) Data subjects and Type of Data
  ◆ (3) Data flow
  ◆ (4) Security measures
  ◆ (4) Contact persons

• Data Protection Policies and Security Measures

• Rights of Data Subject

• Regular review and Monitoring
TRAINING AND CAPACITY BUILDING

Villupuram nurses jump on to technological bandwagon at http://www.thehindu.com/news/national/tamil-nadu/villupuram-nurses-jump-on-to-technological-bandwagon/article5699852.ece
PHYSICAL SECURITY MEASURES
Records room and work stations should have limited access.

Laptops containing 3.7 million Hong Kong voters’ data stolen after chief executive election

Devices contained ID card numbers, addresses and mobile numbers

PUBLISHED: Tuesday, 28 March, 2017, 12:30am
UPDATED: Tuesday, 28 March, 2017, 1:42am
Secure against natural disasters, power disturbances, external access, and other similar threats.
TECHNICAL SECURITY MEASURES
Technical Security Measures

• There is a need for security measures that can easily be implemented to strengthen data processing systems.
Ransomware Hijacks Hotel Smart Keys to Lock Guests Out of their Rooms

Saturday, January 28, 2017  Mohit Kumar

What’s the worst that could happen when a Ransomware hits a Hotel?

Recently, hundreds of guests of a luxurious hotel in Austria were locked in or out of their rooms when ransomware hit the hotel’s IT system, and the hotel had no choice left except paying the attackers.

Available at http://thehackernews.com/2017/01/ransomware-hotel-smart-lock.html
Technical Security Measures

SECURITY POLICY
SYSTEM MONITORING

SAFEGUARDS:
ENCRYPTION,
AUTHENTICATION
PROCESS

INCIDENT
RESPONSE,
CORRECT AND
MITIGATE BREACH,
RESTORE SYSTEM
<table>
<thead>
<tr>
<th><strong>BREACH NOTIFICATION</strong> (<a href="mailto:complaints@privacy.gov.ph">complaints@privacy.gov.ph</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What is subject to the notification requirements.</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Who should notify.</strong></td>
</tr>
<tr>
<td><strong>When should notification of Commission be done.</strong></td>
</tr>
<tr>
<td><strong>When should data subjects or individuals be notified.</strong></td>
</tr>
</tbody>
</table>
What should the notification contain?

1. Nature of breach
2. Personal data involved
3. Measures taken by the entity to address breach
4. Measures taken to reduce harm or consequences of breach
5. Representatives of PIC from whom the data subjects can inquire about the situation
6. Assistance to be provided
WHY SHOULD PERSONAL DATA BE PROTECTED?
<table>
<thead>
<tr>
<th>CRIME</th>
<th>Description</th>
<th>IMPRISONMENT</th>
<th>FINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing of Personal/Sensitive Information for Unauthorized Purpose</td>
<td>Processing information when purpose not authorized</td>
<td>1yr 6mos – 7 years</td>
<td>Php500,000 to Php2,000,000</td>
</tr>
<tr>
<td>Access to Personal/Sensitive Information due to Negligence</td>
<td>Persons who provide access due to negligence shall be liable</td>
<td>1-6 years</td>
<td>Php500,000 to Php4,000,000</td>
</tr>
<tr>
<td>Concealment of Security Breach</td>
<td>Duty to notify Privacy Commission in case of breach</td>
<td>1yr 6mos – 5 years</td>
<td>Php500,000 to Php1,000,000</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>Negligently dispose, discard or abandon personal data of an in an area accessible to the public or placed in its container for trash collection.</td>
<td>6 months – 3 years</td>
<td>Php 100,000 to Php 1,000,000</td>
</tr>
</tbody>
</table>
Can I sue my bank for privacy violation.?

Lake Worth, FL | on May 16, 2012

The teller gave my ex the number of accts I have, under who's name they are, and my balance. This resulted in some assaults on my phone and Facebook which are very degrading. I need to know what to do in that case. He is not listed on my accts. I went to the bank and all they offered is to change my acct and coach the teller...
Four people nabbed in Recto for producing counterfeit documents

Blacklisted workers win £10m payout from construction firms

“During 2008/09 the ICO carried out an investigation into employment blacklisting in the construction industry. As part of that investigation, the ICO seized information from a company called The Consulting Association. Some of the information we seized amounted to a 'blacklist' of individuals who were considered to pose a risk to their employers if employed within the construction industry.”

About £10m will be paid in compensation to more than 250 building workers who were “blacklisted” by some of Britain’s biggest construction firms under a settlement to be announced on Monday.

Cybercrime-based attacks remain the number one cause of data breaches, and they were up 5% to 50% this year, the report says. The rest were rooted in insider woes: 41% via a lost or stolen device and 36% via an “unintentional” employee act. Around 13% cite a malicious insider attack.
HIV status of nearly 800 patients accidentally disclosed by NHS clinic

The disclosure is believed to be the largest of its kind and will likely lead to a major investigation.
A Violation of Privacy is an affront to Human Dignity

Unauthorized use or disclosure may put data subjects at risk for unwanted publicity, discrimination, identity theft and other acts prejudicial to the data subjects.
We are only a little over halfway through 2016, and yet according to the latest IBM X-Force data, 200 million government records worldwide were already compromised by July 31 of this year. That’s nearly 60 million more than all the records compromised from 2013 through 2015 — combined.

GOVERNMENT GOAL

Personal Data

Benefits

Harms
National Privacy Commission Issuances

16-01 SECURITY OF PERSONAL DATA IN GOVERNMENT AGENCIES

16-02 DATA SHARING AGREEMENTS INVOLVING GOVERNMENT AGENCIES

Advisory 17-01
DESIGNATION OF DATA PROTECTION OFFICERS

16-03 PERSONAL DATA BREACH MANAGEMENT

16-04 RULES OF PROCEDURE OF THE NATIONAL PRIVACY COMMISSION
In August, 2016, in a report titled “Data Danger Zones”, the Philippines is ranked as No. 143 out of over 170 nations evaluated on the ability “to keep digital information safe, private and secure.

Available at http://www.telecomasia.net/content/only-four-asian-nations-safe-data-storage
THE PHILIPPINES IS COMMITTED TO PRIVACY AND DATA PROTECTION IN THE GLOBAL DIGITAL ECONOMY
Embracing a Privacy Culture

Thank you!