DATA PROTECTION OFFICER and Data Sharing

IVY D. PATDU
Deputy Privacy Commissioner
National Privacy Commission
Why should Privacy Matter?
A GLOBAL COMMUNITY WITHIN REACH
“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
Pole identified 25 products that when purchased together indicate a woman is likely pregnant. The value of this information was that Target could send coupons to the pregnant woman at an expensive and habit-forming period of her life.

Personal Data Protection

Benefits

Harms
Principle of Accountability
(Data Privacy Act, Section 21)

• Each personal information controller is responsible for personal information under its control or custody.

• The personal information controller is accountable for complying with the requirements of this Act.

• The personal information controller shall designate an individual or individuals who are accountable for the organization’s compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.
DESIGNATE A DPO (and COP)

DPA, Sec. 21; IRR, Sec. 26(a), 50(b);
Circular 16-01, Sec. 4;
Advisory 17-01.
DPO and COP

• Personal Information Controllers and Personal Information Processors shall designate a **Data Protection Officer (DPO)**.

• Functions may be outsourced but DPO must oversee performance. The DPO also remains to be responsible for coordinating with NPC.
Qualifications of a Data Protection Officer

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

• Relevant privacy or data protection policies and practices
• Processing operations
• Sector or Industry

Independent
Knowledgeable
Reliable
"If you want to go fast go alone. If you want to go far, go together."

African proverb

Picture available at https://artofsafari.travel/blog/wisdom-african-proverbs/ (last accessed October 20, 2017)
Getting Started

• Organizational Commitment
  ❑ Register (Phase I Registration)
  ❑ Communicate Designation of DPO
  ❑ Establish Reporting Lines
  ❑ Provide Resources and Support
  ❑ Consider establishing a privacy network
Duties of the DPO

• Monitor compliance

1. Collect and maintain records of processing activities
2. Check compliance
3. Advise and issue recommendations
DATA PRIVACY ACT

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

Uphold Rights of Data Subject

PROPERTY OF THE NATIONAL PRIVACY COMMISSION
NOTICE

TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY

PROPERTY OF THE NATIONAL PRIVACY COMMISSION
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
Organizational
Physical
Technical

Confidentiality
Integrity
Availability
Documents containing Personal Data placed in these lockers for intended recipients.
The recipients' email addresses, of which 730 contained people's full names, were entered into the "to" field instead of "bcc", which masks the email addresses of people receiving the message.
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
Duties of the DPO

• Monitor compliance
4. Maintain accreditations and certifications
5. Advice on need for data sharing agreements
Data Sharing in the Private Sector

1. Data subject must consent to the data sharing even when data is to be shared with an affiliate or mother company.

2. Data sharing for commercial purposes shall be covered by a Data Sharing Agreement.
Are you providing ACCESS to personal data you have collected to a third party? Is it under an outsourcing contract?

Is there a specific provision of LAW that specifically requires data sharing? (Ex. Reporting under R.A. No. 9510 – CISA)

If there is no specific provision of law, is there a public service and a STATUTORY MANDATE? Do you have CONSENT of the data subject?
Contents of Data Sharing Agreements

• Purpose of Data Sharing, including the Public Function and Public Service it facilitates
• Parties to the agreement
• Term or Duration of the Agreement
• Overview of operational details and general description of security measures
• How data subjects can exercise their rights
• 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.
Selling Personal Information without consent

• An example of very common privacy violation by Bank of America was reported by the Utility Consumers' Action Network. In the case Bank of America was charged for selling the personal information (social security numbers, bank account numbers etc) of 35 million customers to marketers and third parties without informing individuals. Bank of America is now settling for $14 million, and agreeing to change its privacy polices, its Web site, and its privacy procedures.

Source: http://cis-india.org/internet-governance/blog/privacy/privacy-banking
Duties of the DPO

- Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP.
Duties of the DPO and COP

• Ensure proper Breach management
• Cultivate Privacy Awareness
• Policy Development and Review
TRAINING AND CAPACITY BUILDING

Photo from National Privacy Commission FB page
Sign up to our monthly newsletter for your chance to win a $50 Airtasker voucher.
Duties of the DPO

• Advice the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights

• Contact person of data subjects, other authorities and NPC
His modus operandi is to steal his victims’ information and then contact call centers of certain banks to request for credit card replacement.
Target to pay $18.5M for 2013 data breach that affected 41 million consumers

Using the credentials to exploit weaknesses in Target's system, the attackers gained access to a customer service database, installed malware on the system and captured full names, phone numbers, email addresses, payment card numbers, credit card verification codes, and other sensitive data.
THANK YOU!

#PartnersForPrivacy