“the right to be let alone - the most comprehensive of rights and the right most valued by civilized men”

[Brandeis J, dissenting in Olmstead v. United States, 277 U.S. 438 (1928)].
Which of the following will you share with a stranger?

- Browsing History
- Diary
- Credit Card Billing Statement
- Home Address
- Messages
- Password
- Phone
- Facebook
Those who process Personal Data

Data Subjects

National Privacy Commission

Processing of Personal Data

• PERSONAL INFORMATION CONTROLLERS (PIC) and PERSONAL INFORMATION PROCESSORS (PIP) PROCESSING PERSONAL DATA of DATA SUBJECTS
PERSONAL DATA

• Any information from which the identity of an individual is apparent
• Any information that can be put together with other information to reasonably and directly identify an individual
• Includes sensitive personal information such as your health, education, genetic or sexual life
• Includes information that is classified or privileged
The agency or corporation who controls the processing of personal data, the one who decides.

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.

Not the employee, Not the data protection officer, Not the Chief Information Officer.
PERSONAL INFORMATION PROCESSOR

• Individual, Corporation or other body who processes the personal data for a Personal Information Controller

• Personal information processor should not make use of personal data for its own purpose

Picture from http://www.livemint.com/Industry/hdDwofLyBZc0XQI0bb70hO/BPOs-edge-towards-highend-work-in-changing-market.html
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
If It’s NOT CLEAR
It’s NOT Consent
Sometimes, consent is NOT necessary...

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

- Law/Regulation
- Sensitive Personal Information
- Provided to government under legal mandate
- To protect life and health
- Protection of rights in court

SUBPOENA
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
The determination of the appropriate level of security must take into account the **nature** of the personal data to be protected, the **risks** represented by the processing, the **size of the organization** and complexity of its **operations**, current **data privacy best practices** and the **cost** of security implementation.
1. Appoint Your Data Protection Officer
2. Conduct Your Privacy Impact Assessment
3. Create Your Data Privacy Manual
4. Implement Data Privacy and Security Measures
5. Be Ready In Case of Data Breach
Technical Security Measures

SECURITY POLICY
SYSTEM MONITORING

SAFEGUARDS:
ENCRYPTION,
AUTHENTICATION
PROCESS

INCIDENT RESPONSE,
CORRECT AND
MITIGATE BREACH,
RESTORE SYSTEM
WHY SHOULD PERSONAL DATA BE PROTECTED?
<table>
<thead>
<tr>
<th>CRIME</th>
<th>IMPRISONMENT</th>
<th>FINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing of Personal/Sensitive Information for Unauthorized Purpose</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>1-6 years</td>
<td>Php500,000 to Php4,000,000</td>
</tr>
<tr>
<td>Concealment of Security Breach</td>
<td>1yr 6mos – 5 years</td>
<td>Php500,000 to Php1,000,000</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>6 months – 3 years</td>
<td>Php 100,000 to Php 1,000,000</td>
</tr>
</tbody>
</table>
Four people nabbed in Recto for producing counterfeit documents

Verizon responds to breach that affected millions of customer accounts.

TalkTalk has today said it will take a hit of up to £35m after last month’s data breach. The attack saw the details of 156,959 customers (including names, emails and phone numbers) and 15,656 bank account numbers accessed by hackers.

Healthcare Suffers Estimated $6.2 Billion In Data Breaches

Nearly 90 percent of healthcare organizations were slammed by a breach in the past two years.

The 911 call has come in loud and clear for the healthcare industry: nearly 90% of all healthcare organizations suffered at least one data breach in the past two years with an average cost of $2.2 million per hack.

Update: TalkTalk offers compensation for data breach - but is it enough?
PRIVACY AND DATA PROTECTION

Benefits

Harms
THE PHILIPPINES IS COMMITTED TO PRIVACY AND DATA PROTECTION IN THE GLOBAL DIGITAL AGE