17/11/2022 (Day 2)  
  
SPI refers to race ethinic origin color marital status age

School   
age   
ID

**Personal information**   
lawful processing of personal data   
contractual  
consent   
legitimate interest -

Performance of an official of public Task- consent is not needed because it is legal action

Protecting vital interests

Compliance with legal obligating   
  
  
SPI

Consent- asking for data subject consent

Lawful and not commercial-   
medical records- health status need to be process by the hospital  
comply with existing laws and regulations  
protect life and health(health or emergency)

EXEMPTIONS  
according to sec 4, DPA of 2012  
applies to the processing of all types of personal information, in the country and even abroad subject to certain qualification  
-if you are involve in money laundrying if you canot hide your personal information pertaining to financial information  
  
  
**need no consent**  
  
sec   
insurance commission   
AMLA  
credit information bureau   
BIR

pic  
banko central  
pip  
landbank

1  
a. Data subjects- people that are applying for ID barnaagy official home owners  
b. PIC bank central/ PIP landbank  
  
2. Personal information   
- name  
- address   
- contact number  
- date of birth  
- email address

Sensitive information   
-blad type  
-bio   
-relogioin  
-marital status  
-sex

3. Security measure

organizational – data policies use firewall - Firewalls are effectively gatekeepers between your computer and the internet  
use security software - You should use security software, such as anti-spyware, anti-malware and anti-virus programs, to help detect and remove malicious code  
  
access control to data processing system   
data base security controls restrict access controlled and audited by internal and external auditors to prevent systems from being used by an authorized persons.  
  
**physical**- add security personnel technical facilitator to assist the participants for example explaioning the procedure like do’s and don’t

improve physical security for example placing CCTV monitoring camera

you can take a picture of your filled up paper or other filled up papers   
  
  
  
proper storation of filled up papers or if not stored proper desposition  
  
  
  
technical – monitor intrusion: You can use intrusion detectors to monitor systems and unusual network activity. If a detection system suspects a potential security breach, it can generate an alarm,   
  
improve physical security for example placing CCTV monitoring camera

back up  
  
trble shooter

Module 3   
  
**5 pillars of compliance – to earn trust mark for PIC and PIP**-appointing a data protection officer   
- Conduct a privacy impact assessment > asses a specific data processing whether if it is qualified of pia or not  
- Develop a privacy management program and privacy manual > Contain the result of PIA   
- Implement data privacy and security measures > you can use ISO standard / cyber security network/ GDPR standard   
- Be ready in case of a data breach > need data breach management team

**Appointing of DPO**- Compliance officer who is responsible for ensuring privacy compliance of the organization   
**Task of DPO** GAPSR  
- assist the PIC/PIP **govern**From operational perspective  
- **Assess** > conduct Privacy impact assessment (PIA)- **Protect** > the organization by developing a Privacy Management Program (PMP)   
 **RTO** recovery time objective **RPO** recovery point objective  
- **Sustain** > conducting audits as well as ensure the ongoing monitoring of risks   
- **Respond** > respond personal data related quarries and complaints especially if there is a personal data   
 breach

**Registration for compliance**

if your company exceed 250 employees above   
handled at least 1000 records  
for decision making PI and SPI  
if you believe is included in your processing  **Compliance checks**

**NPC’S NEW REGISTRATION AND RENEWAL PLATFORM**  
eRehistro

**PRIVACY IMPACT ASSESMENT**   
  
know your risks – section 20.C of DPA of 2012

Purpose of pia is to determine the risks of data privacy

**3 ELEMENTS OF PRIVACY RISK ASSESSMENT** (ACTIVITY) WHILE PIA IS THE TOOL

**Records of processing activities**   
  
**registration**   
  
**privacy impact assessment** WHILE PIA IS THE TOOL  
  
**CONDUCT A PRIVACY IMPACT ASSESSMENT (PIA)**

What compliance look like?

Risks assessments to the privacy rights of the data subjects

* Process inventory is updated including list of process owners
* PIA is conducted and owned by process owners
* Stakeholder are involved
* PIA includes risk map, list of recommended control measure with implementation plan/timelines

Do not take into account the privacy risks of the data subjects

* No PIA
* Process owners do not own the PIA
* PIA not updated
* Stakeholders are not involved
* Recommended controls are not implemented

**PRIVACY IMPACT ASSSESMENT PROCESS**

**DOING PIA**

Who collected what purpose? >

**PRIVACY MANAGEMENT PROGRAM AND PRIVACY MANUAL –** is a

-Strategic framework to build robust infrastructure   
-minimize risk and maximize ability to response to privacy issues   
-demonstrate commitment

**IMPORTANCE OF PMP**

* It puts everyone on the same page > need to involved everyone organizational approach
* Makes compliance more manageable > every works together being the pic and pip
* Gives pics and pip competitive advantage > they will be prepared when they need to act if problems occur
* Help pip pic avoidable expenses

**SECURITY MEASURES IN THE PROCESSINGOF PERSONAL DATA**

Collection/ acquisition > storage > use > disclosure/ transfer > retention/disposal > repeat

5 PILLARS OF COMPLIANCE

1. Dpo
2. PIA
3. PMP
4. PDP

**What compliance looks like**

Data handlers have security

Privacy notice where appropriate e.g website

Data sharing agreements in place

Service providers in compliance

**What negligence looks like?**

Privacy policy sits on shelf

No security clearance or privacy trainig for data handlers

No privacy notice when cpollecting personal data

Over collention

No privacy impact assessment

**PERSONAL DATA BREACH MANAGEMENT**

The PIC shall promptly notify the commission and affected data subjects when sensitive peronal information or other information that may, under the circumtances, be used to enable iedentity fraud are reasonably believed to have been acquired by an unauthorized person, and the PIC or the commission be;lieves that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subejcct

**Section 430 dpa**

**STRUCTURE OF NPC CIRCULAR**

**4 TYPES OF BREACH**

* Availability breach   
  due to loss, accident or unlawful destruction of personal data
* Confidentiality breach   
  due to unauthorized disclosure or or access to personal data
* Integrity breach   
  due to alteration of personal data
* Unlawful processing/Violation of privacy   
  unathorized processing processing for unauthorized purpose violation

**DETAILED CONTENTS OF NPC NOTIFICATION**

**NOTIFICATION OF DATA SUBJECTS, SECTION 18**

**WHO SHOULD NOTIFY?**

Data subject (affected)

**PRIVACY BREACHES EXAMPLES**

**COMPLAINCE IS A JOURNEY**

**COMPLIANCE CHECK**

Scope – who are covered   
>PIP and PIC

**MODES OF COMPLIANCE CHECK**

Privacy sweep – touch point

Documents submission - documents

On site visit – behavior

**NPC COMPLIANCE FRAMEWORK**

**OBEJECTIVE OF PIA**

1. The adherence of the pic or pip to the principle of the transfarecncy legitimate purpose and proportionality
2. The existing organizational, phusical and technical security measures in the data processings system of the pip o
3. Pip pic upholds the right

**PIA EXERCISE – LGU ADMINISTRATION OF POLIO VACCINE**