Information Security and Data Privacy Protection

September 6-8, 2023

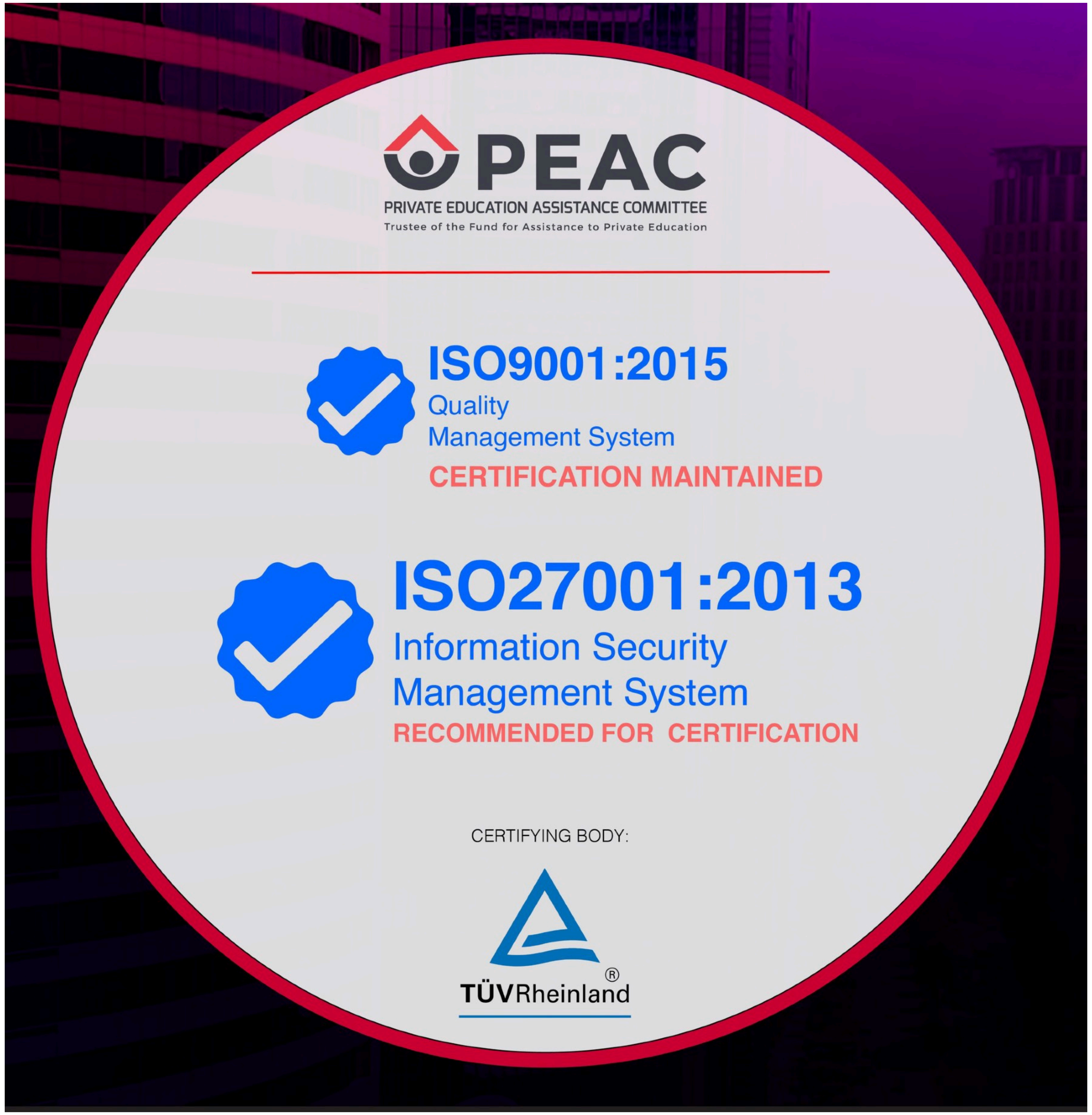
Topics to be covered

PEAC’s Commitment to Strengthen the Implementation and Management of GASTPE Programs

Information Security and Data Privacy Protection

Implementation of Security Measures

Our Commitment to Quality and Information Security



PEAC

PRIVATE EDUCATION ASSISTANCE COMMITTEE

Trustee of the Fund for Assistance to Private Education

ISO9001:2015

Quality Management System

CERTIFICATION MAINTAINED

ISO27001:2013

Information Security Management System

RECOMMENDED FOR CERTIFICATION

CERTIFYING BODY:

TÜVRheinland®

Why do we need to protect personal data?

It builds trust

It prevents and mitigates risk

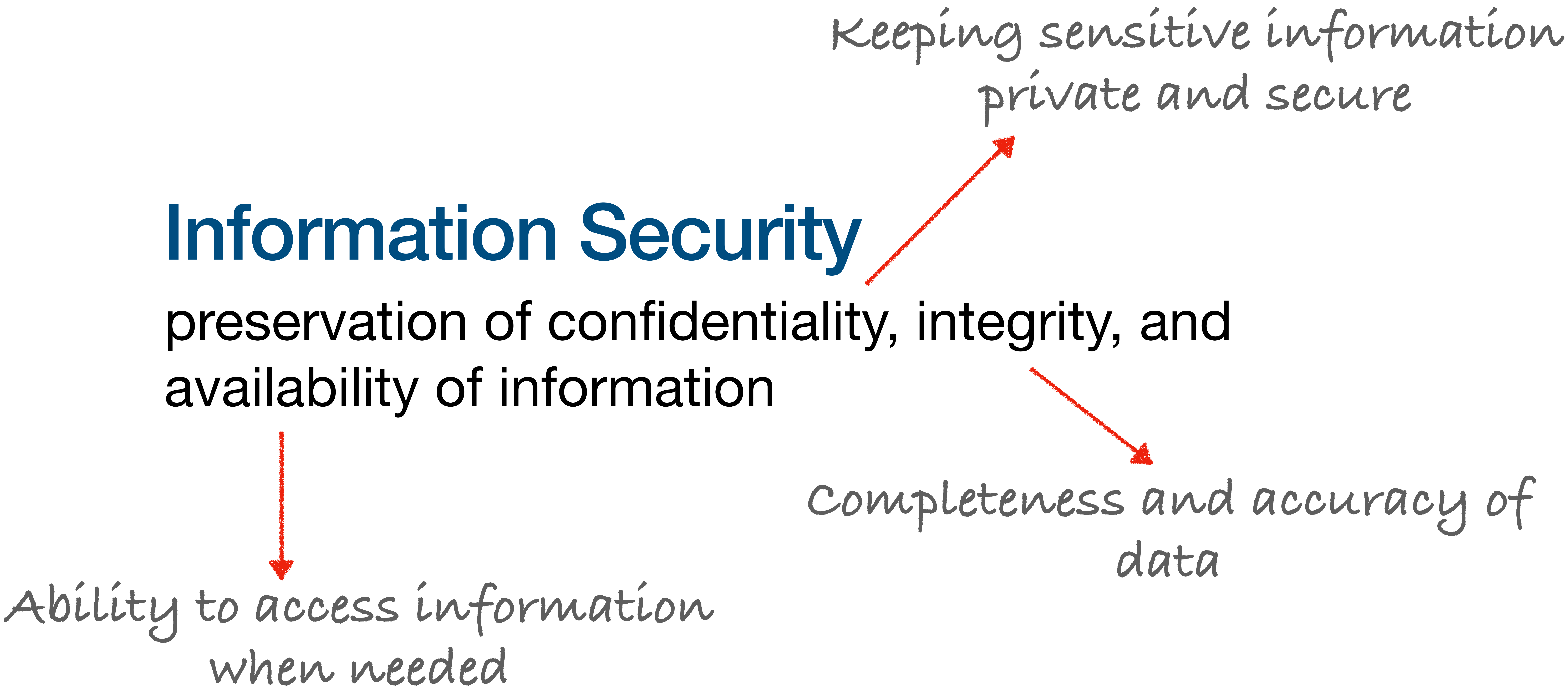
It is required by law

Additional reference: Foundation for Media Alternatives

Data Processed in the EIS, IMS, VMS

3,641 ESC-participating schools
923,314 ESC grantees
49,280 TSS recipients

4,547 SHS VP-participating schools
1,355,135 Voucher Program Beneficiaries



Information Security

preservation of confidentiality, integrity, and availability of information

Keeping sensitive information private and secure

Completeness and accuracy of data

Ability to access information when needed

Republic Act No. 10173

Data Privacy Act of 2012

AN ACT PROTECTING **INDIVIDUAL PERSONAL INFORMATION**

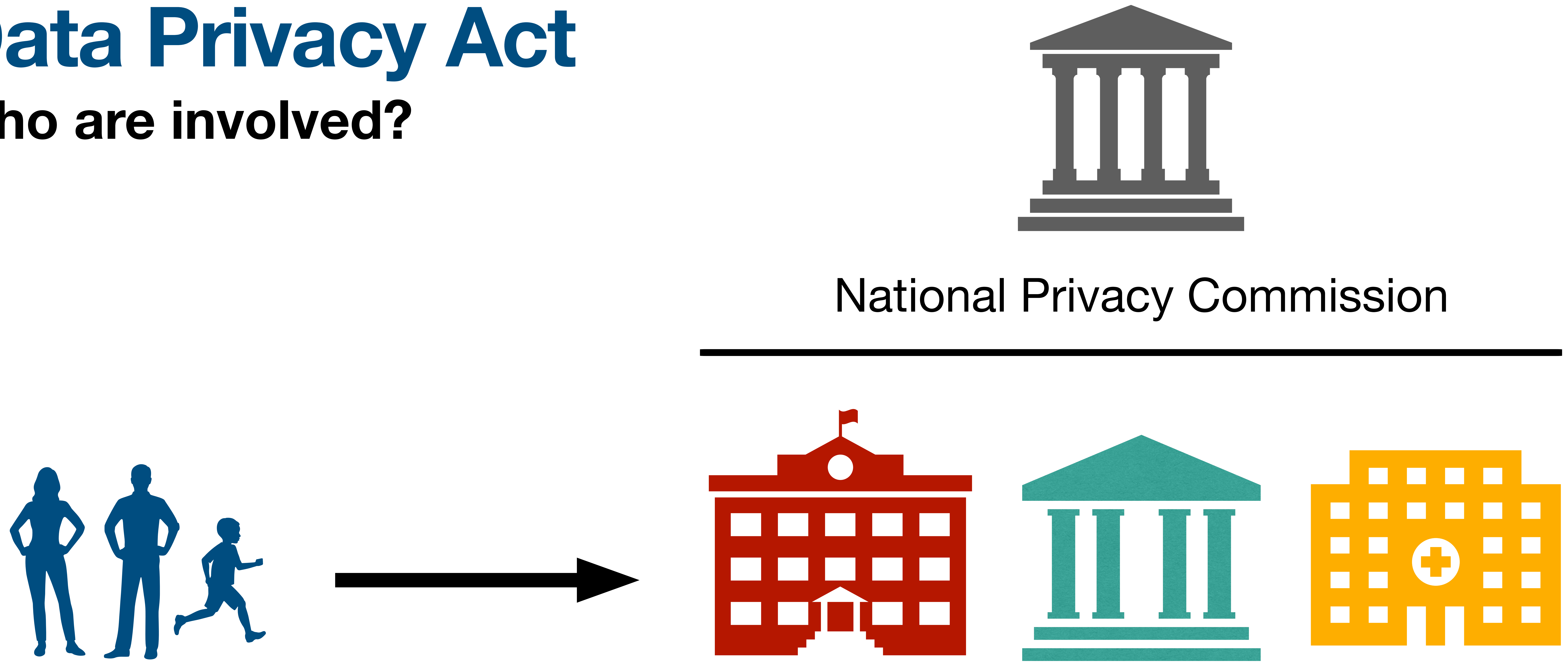
IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR,

CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

Final Implementing Rules and Regulations came into force on September 9, 2016

Data Privacy Act

Who are involved?



National Privacy Commission

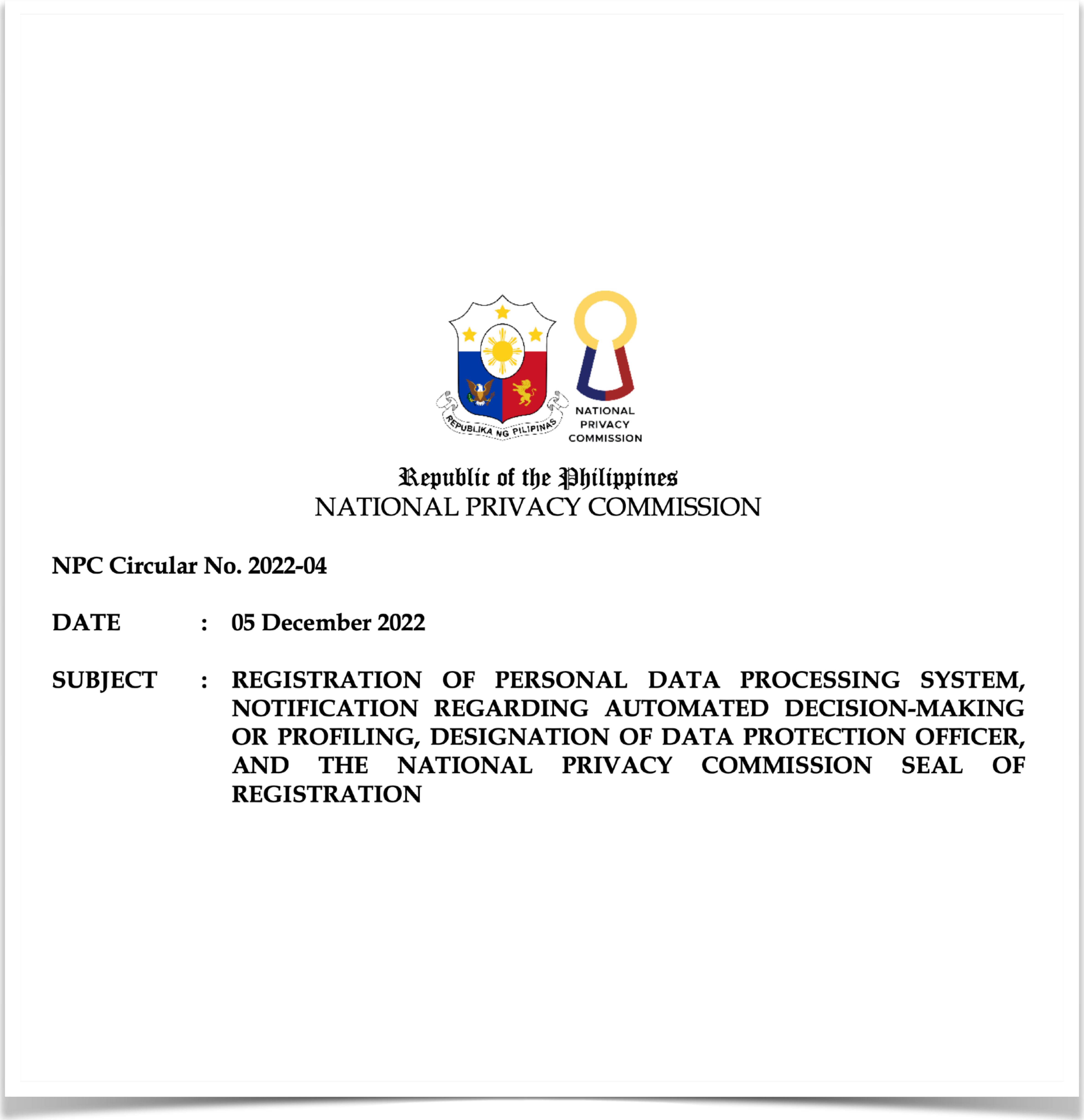
Data Subjects

Personal Information Controller (PIC)
Personal Information Processor (PIP)

Data Privacy Compliance

Data Privacy Act of 2012

- Appointment of a Data Protection Officer
- Registration of Data Processing Systems



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Circular No. 2022-04

DATE : 05 December 2022

SUBJECT : REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION

What is “personal data”?

Personal Information vs. Sensitive Personal Information

Personal Information (PI)

Sec. 3 (g), DPA

PI 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.

Examples:

First name
Last name
Residence
Place of work
Social media handle
Email address
Mobile number
Picture

Sensitive Personal Information

Sec. 3 (l), DPA

SPI 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.

Reveals
- Race, ethnic origin, marital status, age, color,
- Religious, philosophical, and political affiliation

Concerns
- Health
- Education
- Genetic or sexual life
- Proceedings for any offense committed, its disposal, sentence of court arising from such proceeding

Issued by government agencies
- Social security numbers
- Previous or current health records
- Licenses or its denials, suspension, or revocations
- Tax returns

ESC, TSS, and SHS VP

Personal data that we process

- Learner Reference Number
- Full Name
- ESC ID / QVA Certificate Number
- Birthdate
- Gender
- Date of first attendance
- Track and strand
- Tuition fees paid
- Other education data: JHS, ALS, PEPT, Passed G10 when?, Passed G11 when?, previously enrolled?
- PRC License numbers
- Full name of signatories and encoder
- Office
- Contact information
- E-signatures
- Monitoring findings

Internal Use

Processing

Sec. 3 (j), DPA

Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the…

- collection
- recording
- organization
- storage
- updating or modification
- retrieval
- consultation
- use
- consolidation
- blocking
- erasure or destruction of data.

General Data Privacy Principles

Sections 17 and 18, DPA IRR

TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY

Security Incidents and Data Breaches

A **security incident** is any event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that may result in a personal data breach, if not for safeguards that have been put in place.

A **data breach is a kind of security incident**. It happens when there is 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.

Four Types of Breaches

1. **Availability Breach**
   Due to loss, accidental or unlawful destruction of personal data

2. **Confidentiality Breach**
   Due to the unauthorized disclosure of, or access to, personal data

3. **Integrity Breach**
   Due to alteration of personal data

4. **Unlawful Processing / Violation of Privacy**
   Unauthorized processing, processing for unauthorized purposes, violation of privacy rights

Incidents that may lead to a breach

- Shoulder-surfing
- Human error
- Fire
- Flood
- Earthquake
- Image capture
- Phishing

- Ransomware
- Forgery
- Eavesdropping
- Loss of physical files
- Redirection
- Software malfunction
- Hardware malfunction

- Computer system breach
- Unauthorized access to, or use of, systems, software, or data
- Unauthorized changes to systems, software, or data
- Loss or theft of equipment storing institutional data
- Interference with the intended use of IT resources
- Compromised user accounts

Sec. 20 (a) of the DPA states that “The personal information controller must implement **reasonable and appropriate organizational, physical and technical measures** intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.”

Security Measures for the Protection of Personal Data

Sections 25-29, DPA IRR

ORGANIZATIONAL

PHYSICAL

TECHNICAL

Representations and Warranties

By creating this billing statement/registration in behalf of [SCHOOL NAME] I represent and warrant that as of the date of submission of the information regarding the school's [Grantees/Registrants/Participants], consistent with the Data Privacy Act:

1. All the information provided herein are true and correct;
2. Consent of the Data Subjects have been properly obtained in accordance with law with respect to the processing of their personal information;
3. The Data Subjects have been provided with the following information prior to collection or before data is shared;
   - Identity of the Personal Information Controllers of Personal Information Processors that will be given access to their personal data;
   - Purpose of data sharing;
   - Categories of personal data concerned;
   - Intended recipients or categories of recipients of their personal data;
   - Existence of the rights of data subjects, including the right to access and correction, and the right to object;
   - Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

Reminders

Security Incident Reporting

- All information security incidents, whether actual or suspected, shall be reported to the PEAC through email
    - info.security@peac.org.ph
    - data.privacy@peac.org.ph

Thank you.