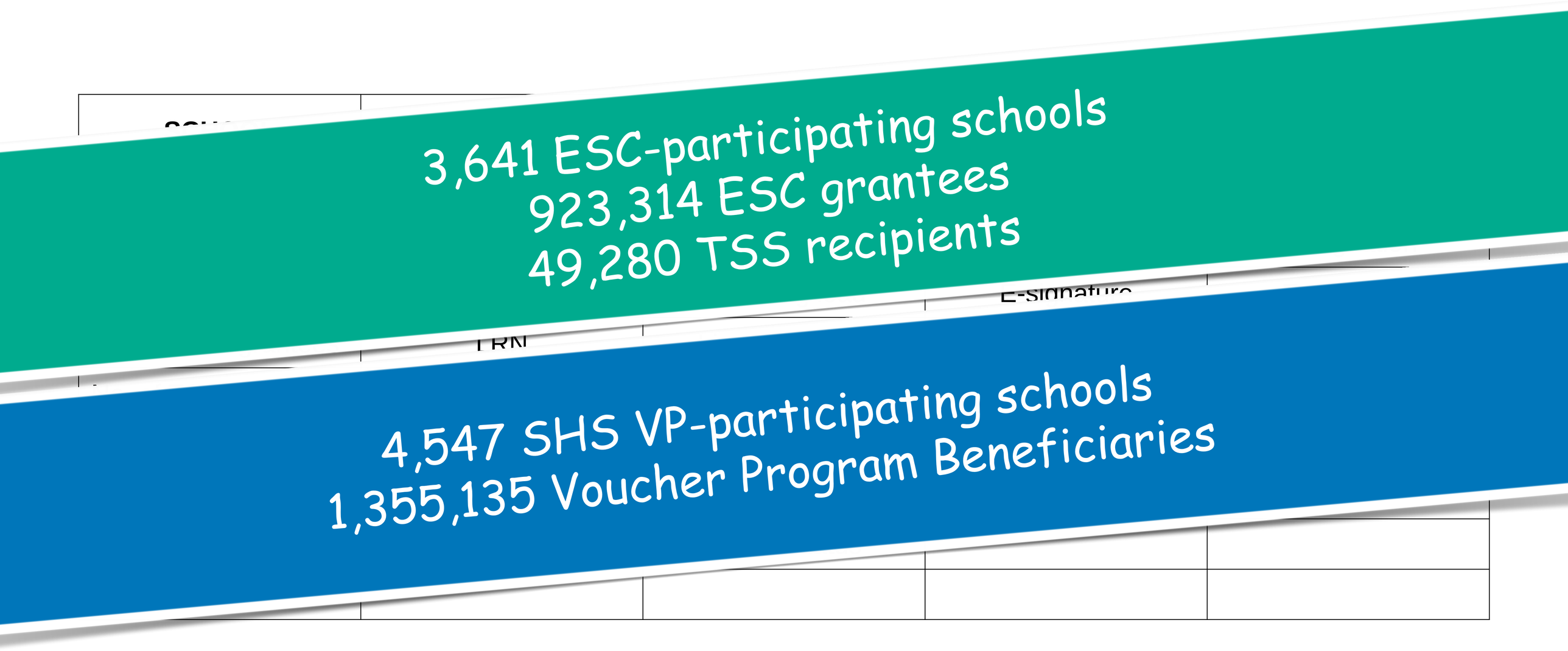
Information Security and Data Privacy Protection

To be covered

- PEAC’s Commitment to Strengthen the Organization
- Data Privacy Compliance
- Reminders on secure access to PEAC’s systems and information assets; security incident reporting
- Push towards effective data governance

Commitment to strengthen the organization

Data Processed in the EIS, IMS, VMS



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
Favorite food
Social media handle
Email address
Mobile number

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

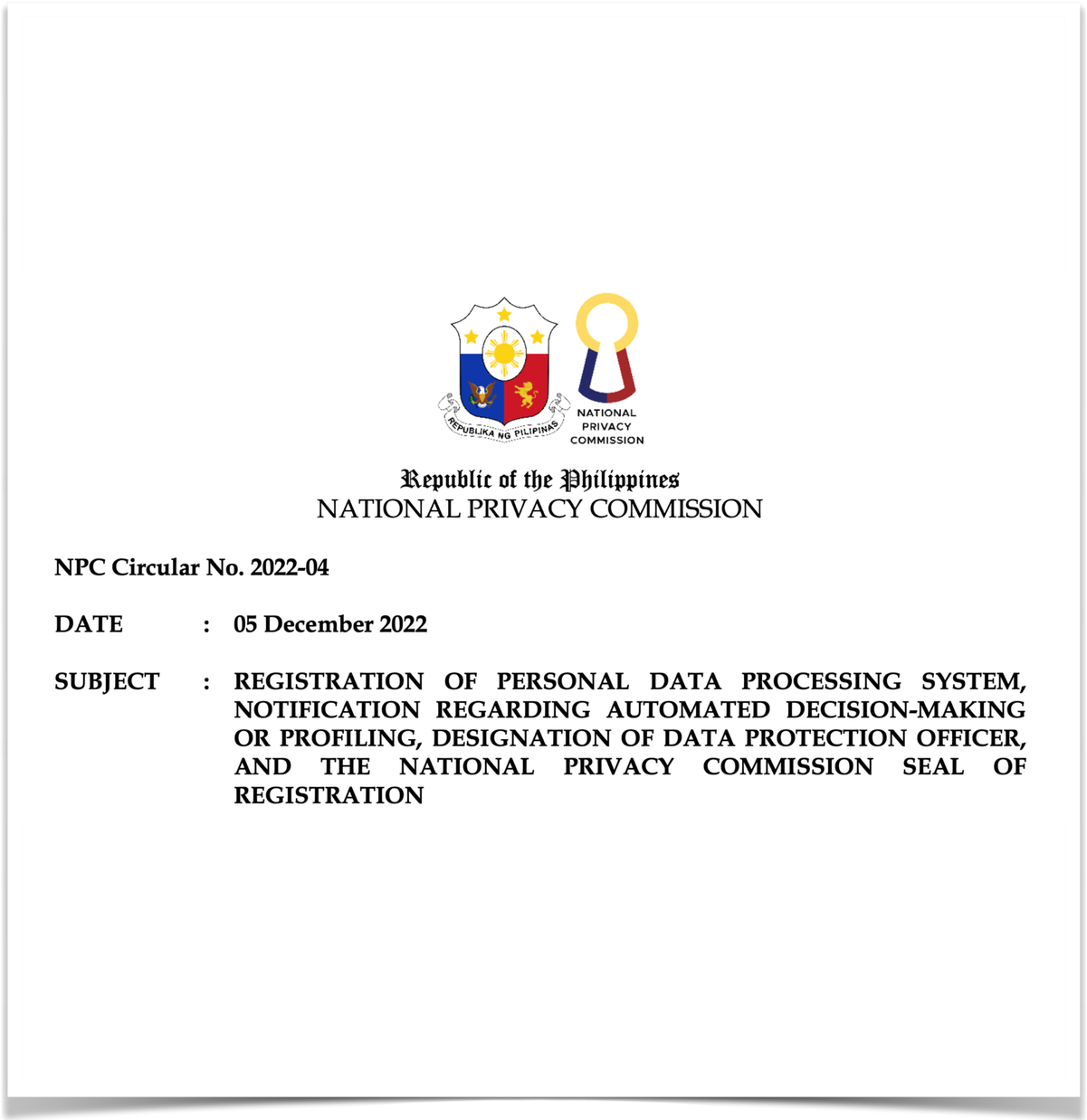
Concerns
- Health
- Education
- Genetic or sexual life
- Proceedings for any offense committed, its disposal, sentence of court arising from such proceeding

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

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

Mandatory Registration

Sec. 4 (A), NPC Circular. 2022-04

Registration of an entity's Data Processing System and DPO with the Commission shall be one of the means through which a PIC or PIP demonstrates its compliance with the DPA, its IRR, and other relevant issuances of the NPC.

Mandatory Registration

Sec. 5, NPC Circular. 2022-04

A Personal Information Controller (PIC) or Personal Information Processor (PIP) that

- employs two hundred fifty (250) or more persons, or
- those processing sensitive personal information of one thousand (1,000) or more individuals, or
- those processing data that will likely pose a risk to the rights and freedoms of data subjects

shall register all Data Processing Systems.

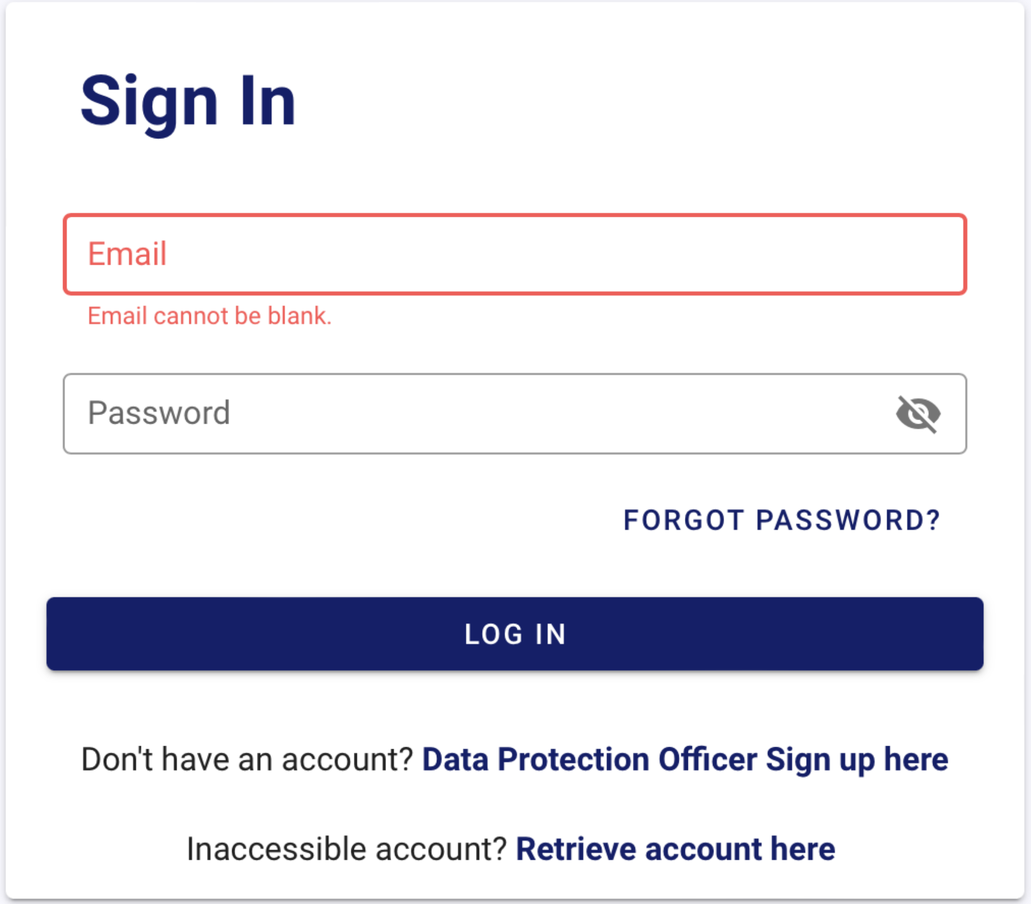
Mandatory Registration

Sec. 13, NPC Circular. 2022-04

NPC shall issue a Certificate of Registration in favor of a PIC or PIP, that has successfully completed the registration process. The validity of the registration is one year from its date of issuance.

NATIONAL PRIVACY COMMISSION

https://npcregistration.privacy.gov.ph/login



NATIONAL PRIVACY COMMISSION

Private Education Assistance Committee
PIC/PIP

- Home
- Dashboard

Main Menu

- Data Breach Notification
- Annual Security Incident Report

Hello, Eimann Evarola!

Welcome to DBNMS!

CREATE PDBN

CREATE ASIR

Unsure of what form to create? Undergo Self Assessment here

Appointment of a Data Protection Officer

Pillar of Compliance

Image source: National Privacy Commission

Reminders

Secure access to PEAC’s information systems (data processing systems)

- Review the list of authorized personnel who has access to your school’s EIS, IMS, Certification System, and SHS VMS accounts
- During registration, ensure that email accounts entered into the system are accessible, preferably not a personal email account
- De-register a user immediately when he/she no longer connected with the school
- A Non-disclosure Agreement (NDA) that has provisions on protection of proprietary information and data privacy protection executed by authorized personnel would add additional protection

Reminders

Secure access to PEAC’s information systems (data processing systems)

- Enable Two-Factor Authentication
- Use secure passwords (we recommend using at least 12 characters, alpha numeric + special characters)
- Change passwords at least once a year (we recommend changing your passwords every three months)
- Do not use public terminals when accessing the EIS, CS, IMS, VMS
- Refrain from using public Wifi
- Logout of your account properly

PEAC
PRIVATE EDUCATION ASSISTANCE COMMITTEE
Trustee of the Fund for Assistance to Private Education

Home | A.Y: 2022 - 2023 | 

Welcome to PEAC Enterprise Information System (EIS)

PEAC Test School

ESC ID: '

Account Profile | Security & Login | User Management

STATUS

(RE) CERTIFICATION	MONITORING VISIT	ATTENDANCE IN THE ANNUAL GASTPE ORIENTATION
Limited Compliance	To be Updated	Did Not Attend

Share Your Feedback

SCHOOL INFORMATION

UPDATE SCHOOL INFO

DEPED ID:	
REGION:	
OFFICIAL EMAIL ADDRESS:	
TELEPHONE NO.:	

QUICKLINKS

RECENT ACTIVITY

VIEW ACTIVITY

USERS

MANAGE USERS

← Back

Change Password

2-Factor Authentication

2-FACTOR AUTHENTICATION

Two-Step Verification is already enabled. You will receive an authentication code when you sign in. Authentication codes will be sent to your registered mobile number.

ENABLE 2-FA

MOBILE NUMBER

+63

Update Mobile Number

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

Reminders

Security Incident Reporting

- The report shall include
  - Nature of the information security incident/data breach
  - Date and time the incident/breach was discovered
  - Information assets/personal data involved
  - Compromised information asset / Data subjects involved
  - Initial actions undertaken

Push for effective data governance

Thank you.