Infosec and Data Privacy Protection

GASTPE Orientation Conferences

Butch Evarola | July, 2024

Jun 7, 2024

INQUIRER.NET

Today's

NPC issues show cause orders to 65 tenants of a Parañaque mall

By: Alden M. Monzon - @inquirerdotnet Philippine Daily Inquirer / 09:43 AM May 16, 2024

MANILA, Philippines — The National Privacy Commission (NPC) on Wednesday said it found 65 stores inside a mall in Parañaque that registered with them or had other violations, prompting them to issue notices to these shops, kiosks, and booths which process personal information.

The NPC said it held its first-ever compliance sweep at the mall as assessment of the compliance of these establishments with the requirements under the Data Privacy Act (DPA).

June 07, 2024 11:07 am Manila +29°C

MANILA BULLETIN

NEWS BUSINESS ECONOMICS OPINION ENTERTAINMENT SPORTS TECHNOLOGY LIFESTYLE SPECIALS

Up to P5-M maximum administrative fine for non-compliance with NPC orders

BY SONNY DAANOY

May 16, 2024 09:41 AM

The National Privacy Commission (NPC) reminded owners, especially inside the malls, to ensure their businesses are registered and compliant with the Commission's regulations.

NPC Commissioner John Henry Naga and other officials during the on-the-spot privacy sweep in Ayala Malls Manila Bay on Wednesday, May 15, 2024. (Photo from NPC)

Breach Handling

National Privacy Commission

Common causes of data breach incidents:

- Human Error
- Malicious Attack
- System Glitch

ESC CERTIFICATION ASSESSMENT INSTRUMENT USER'S GUIDE

Area E
Registrar's Office

II. Registrar's Office			
1. Established policies and procedures for safekeeping, retrieval, retention and disposal of students' records according to the Data Privacy Act*	- Do the records management SOPs comply with the Data Privacy Act?	- Compliance with Data Privacy in records management particularly in Safekeeping, Retrieval, Retention and disposal	- Registrar's Office SOPs/ Handbook/Manual - Administration Manual - Data Privacy Policies and Protocols

Area E
Guidance and Counseling

6. A system for maintaining confidentiality of students' data and information	- Are students' information records kept confidential and managed properly according to Data Privacy Act?	- Confidentiality of Student Information and Record	- Student Information and Records Management SOPs - Guidance Center Handbook/ Manual

Security of Personal Data in the Government and Private Sector

NPC Circular 2023-06

All Personal Information Controllers must implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal data.

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.

Sensitive Personal Information (SPI)

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;

Sensitive Personal Information (SPI)

Sec. 3 (l), DPA

SPI refers to personal information:

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.

General Obligations of PICs and PIPs

NPC Circular 2023-06

https://npcregistration.privacy.gov.ph

1. Designation and registration of a Data Protection Officer with the National Privacy Commission.
2. Registration of data processing systems with the NPC
3. Creation of an inventory of all data processing systems and activities

General Obligations of PICs and PIPs

NPC Circular 2023-06

4. Conducting a Privacy Impact Assessment on the processing of personal data

5. Setting up a Privacy Management Program

6. Periodic training of employees, agents, personnel, or representatives on privacy and data protection policies.

Embedding Privacy-by-design and Privacy-by-default

NPC Circular 2023-06

Storage of Personal Data

NPC Circular 2023-06

General Rule: A PIC or PIP must store personal information in a form that permits the identification of data subjects for only as long as necessary for the specific purpose for which it was initially processed.

Access to Personal Data

NPC Circular 2023-06

There should be an Access Control Policy to ensure that only authorized personnel can access personal data on a “need to know” basis.

Implement secure authentication mechanisms, such as multifactor authentication or secure encrypted links, when providing personnel online access to sensitive personal information, privileged information, and a high volume of personal data.

Business Continuity Management

NPC Circular 2023-06

A PIC or PIP must have a Business Continuity Plan to mitigate potential disruptive events.

Transfer of Personal Data

NPC Circular 2023-06

Emails

Removable or Portable Storage Media

Fax Machines

Transmittal

Disposal of Personal Data

NPC Circular 2023-06

Disposal and Destruction of Personal Data - In establishing policies and procedures for disposal of personal data

- Retention period of data;
- Jurisdiction-specific laws, regulations, and existing contracts;
- Identification of relevant de-identification, anonymization, or deletion techniques for specific types of data; and
- Required documentation before the deletion, de-identification, or anonymization of personal information.

Other information

NPC Circular 2023-06

Threat monitoring and vulnerability management.

Personal Data Breach Management.

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

Reminders

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

- 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)

Reminders

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

- Do not use public terminals when accessing the EIS, CS, IMS, VMS
- Refrain from using public Wifi
- Logout of your account properly

Thank You!

Key Components of Information Security