Government and Private Sector Privacy

Francis Euston R. Acero
Complaints and Investigations Division

10 August 2017

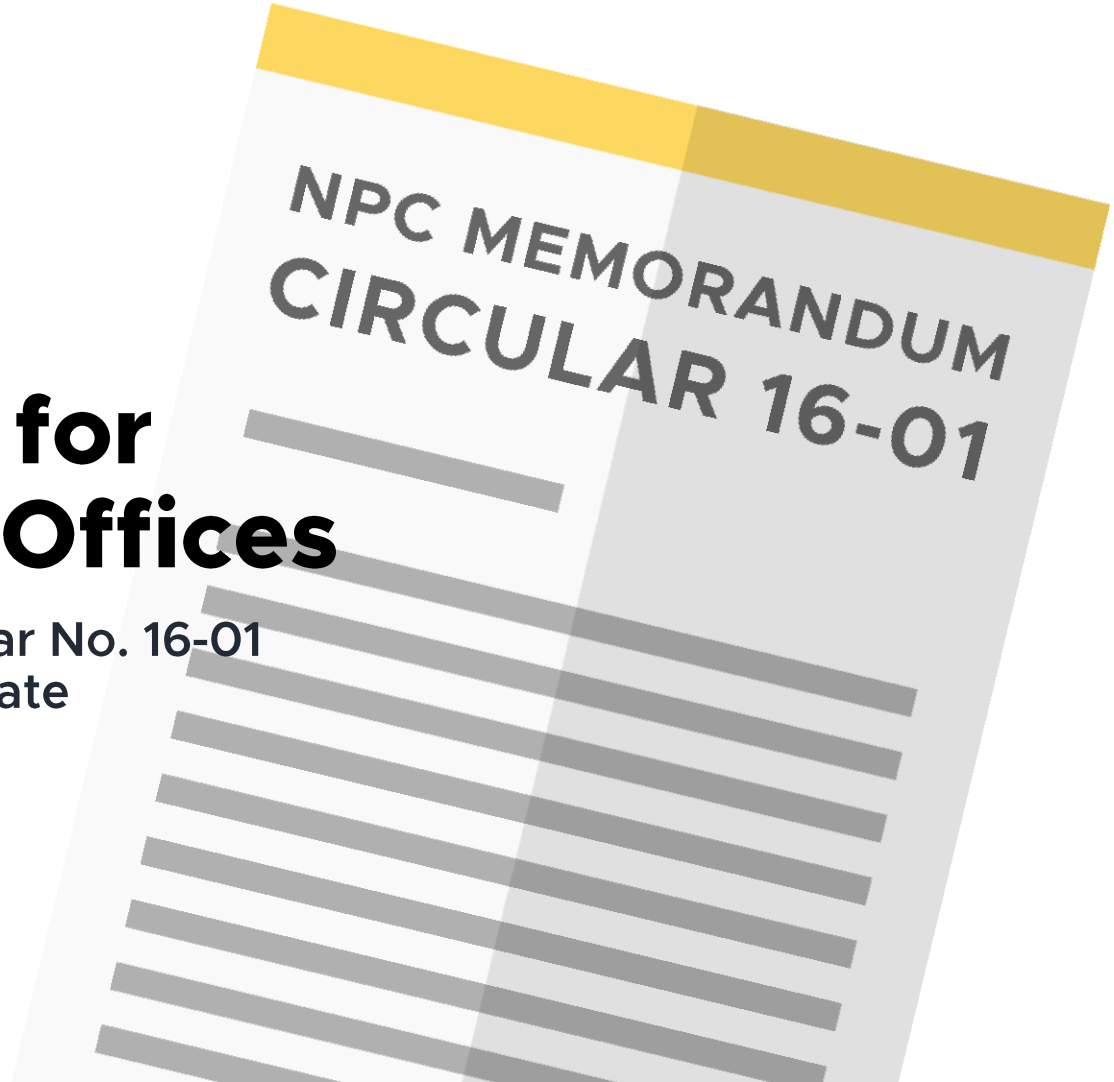
NATIONAL PRIVACY COMMISSION

In this presentation

- Data Privacy Standards for Government Offices
- Sectoral Champions and Sectoral Codes
- The Data Protection Officer

NATIONAL
PRIVACY
COMMISSION

NATIONAL
PRIVACY
COMMISSION



Data Privacy for Government Offices

Understanding NPC Circular No. 16-01 and what it means for private corporations

General Obligations

NATIONAL PRIVACY COMMISSION

- Designate a Data Protection Officer
- Conduct a Privacy Impact Assessment (NPC Advisory No. 17-03), and update as often as necessary
- Create privacy and data protection policies
- Conduct organization-scale training on privacy and data protection policies.
- When appropriate, register the system.
- Cooperate when policies are subjected to assessment.

The Privacy Impact Assessment

NATIONAL PRIVACY COMMISSION

Data Inventory

- Identifies types of personal data held by the agency, including employee records
- All information repositories holding personal data, including location
- Assessment of necessity and proportionality of processing in relation to purpose of processing
- Assessment of the risks to the rights and freedoms of data subjects

Control Framework

NATIONAL PRIVACY COMMISSION

- Addresses risks identified in the PIA
- Enumeration of measures, includes organization, physical, and technical measures to maintain availability, integrity, and confidentiality
- Protection measures against natural and human dangers
- Includes
  - Nature of personal data to be protected
  - Risks represented by the processing, size of organization, and complexity of operations
  - Best practices
  - Cost of implementation

Storage

NATIONAL PRIVACY COMMISSION

- Must be stored in a data center
- If digitally processed, must be encrypted with at least AES-256 encryption
- Passwords must be strong enough
- Access to all data centers must be restricted to those with appropriate security clearance
- NPC may audit, or may be independently verified or certified

Agency Access to Personal Data

NATIONAL PRIVACY COMMISSION

- Only programs developed or licensed by a government agency may access or modify databases containing personal data under that agency's control
- Access must be strictly regulated
- Contractors, consultants and service providers may access only pursuant to strict procedures in formal contracts
- Each user must sign an agreement explaining an updated acceptable use policy

Agency Access to Personal Data

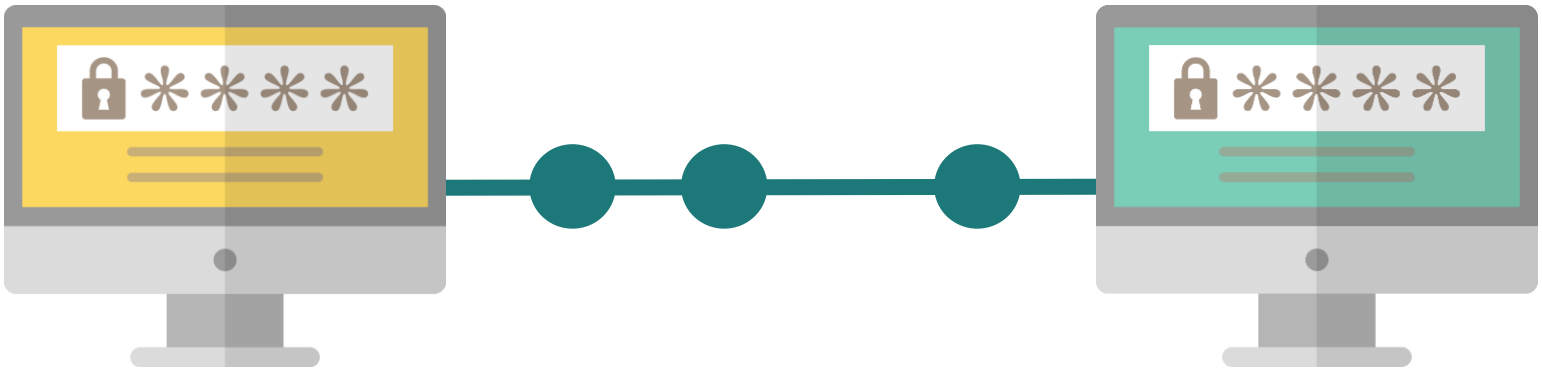
NATIONAL PRIVACY COMMISSION

- Must use multi-factor authentication for online access
- Only known devices, properly configured for security, can access personal data. Only authorized media may be used on computer equipment.
- Mobile devices owned by the agency must be equipped with remote disconnection or deletion technologies.
- Paper-based data systems must keep logs showing file last accessed, including when, where, and by whom.

Transfer of Personal Data

NATIONAL PRIVACY COMMISSION

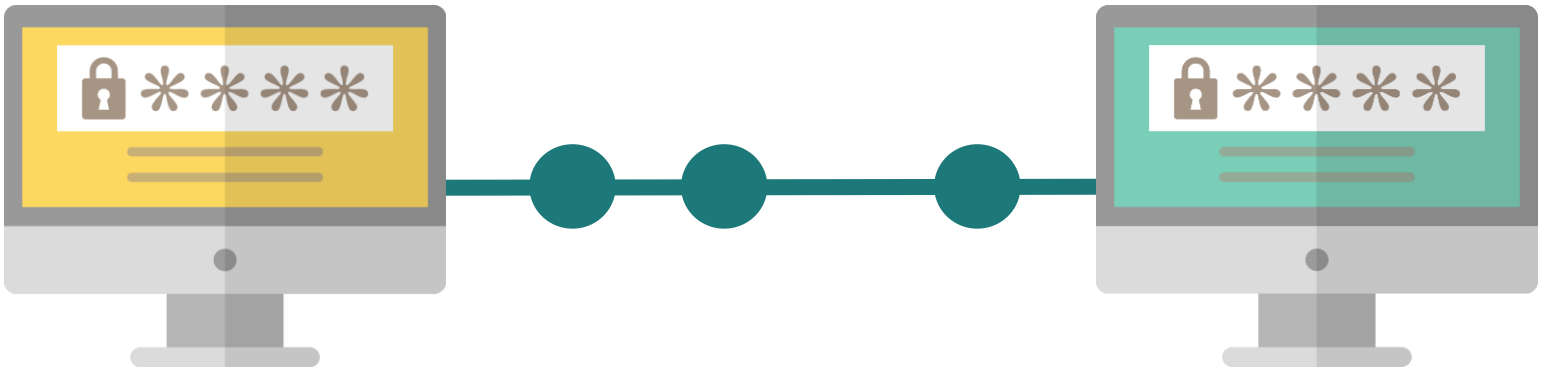
- If done by e-mail, must ensure that data is encrypted, or use a secure e-mail facility that facilitates the encryption of all data, including any attachments.
- Send passwords on a separate e-mail.
- Scan outgoing emails for attachments and keywords that indicate personal data, and prevent transmission



Transfer of Personal Data

NATIONAL PRIVACY COMMISSION

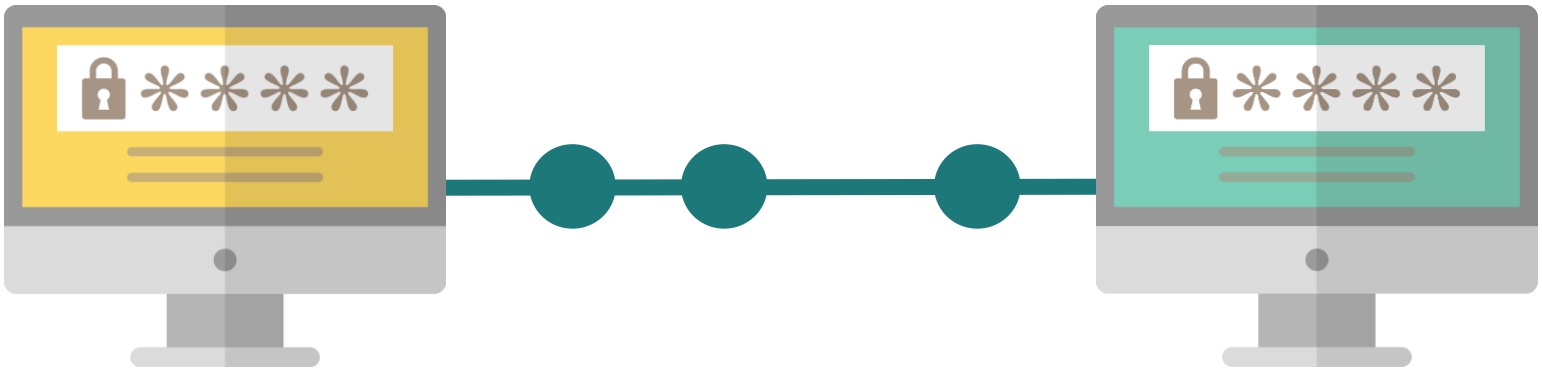
- Controls must be in place to prevent printing or copying to word processors and spreadsheets without security or access controls in place.
- Data stored in portable media, like discs or USB storage, must be encrypted
- Laptops must utilize full disk encryption



Transfer of Personal Data

NATIONAL PRIVACY COMMISSION

- Manual transfer of personal data, where possible is prohibited. If impossible, authentication technology must be in place.
- NO FAX TRANSMISSIONS
- Use registered mail or, where appropriate, guaranteed parcel post service.
- Safeguards apply to internal transfers



Disposal of Personal Data

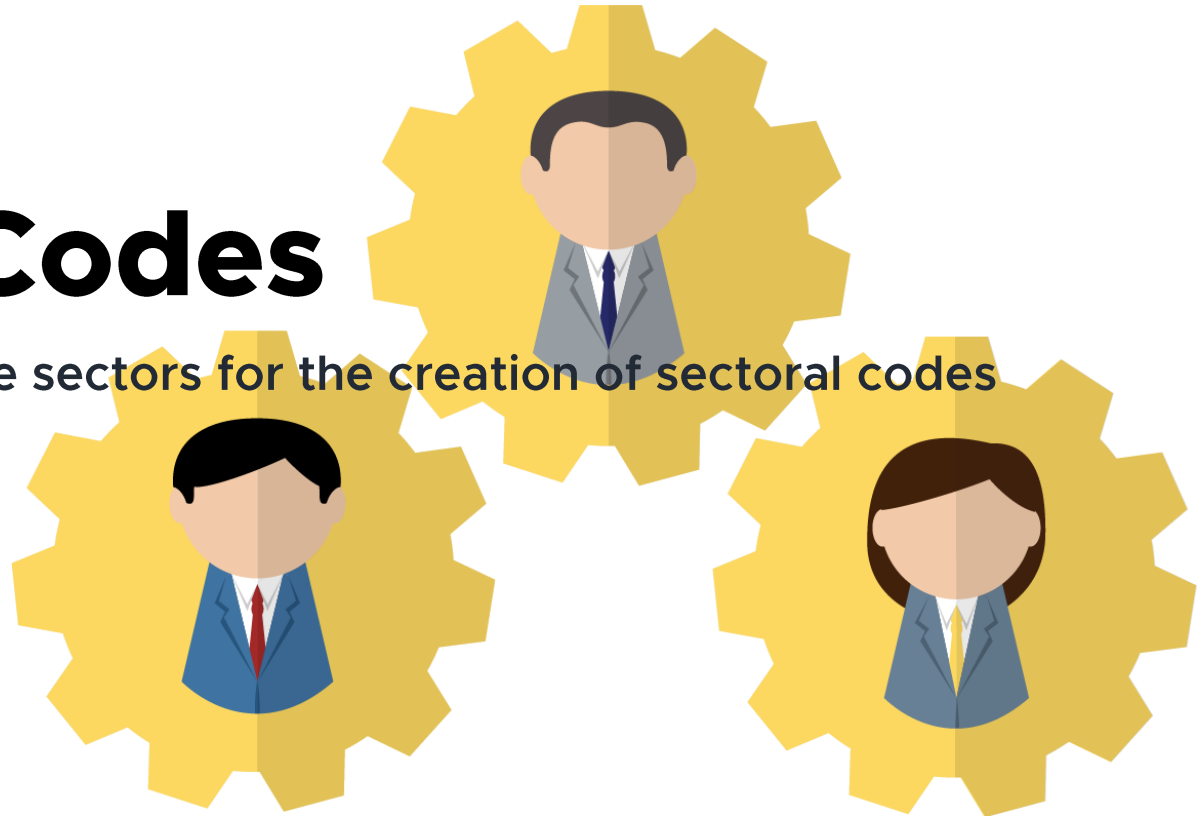
NATIONAL PRIVACY COMMISSION

- All disposal must comply with National Archives of the Philippines Act (RA 9470) if archiving records
- Procedures must be established over:
  - Disposal of files that contain personal data, regardless of storage medium
  - Disposal of computer equipment at end-of-life, including storage media. Includes the use of degaussers, erasers, physical destruction devices
  - Offsite disposal

NATIONAL
PRIVACY
COMMISSION

Sectoral Codes

Engaging with high value sectors for the creation of sectoral codes



Attributes of Effective Privacy Authorities

NATIONAL PRIVACY COMMISSION

- Promote Education and Awareness
- Seek Feedback
- Offer Guidance and Assistance
- Strive for Coordination and Cooperation
- Business and Technology Savvy
- Judicious
- Transparent

Part of Powers and Functions

NATIONAL PRIVACY COMMISSION

- Sec. 7 (j), RA 10173
  - Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers.
  - These privacy codes must adhere to the underlying data privacy principles
  - Privacy codes may include private dispute resolution mechanisms for complaints
  - The Commission may review such privacy codes and require changes

The DPO Forum

NATIONAL PRIVACY COMMISSION

- Means by which the NPC gets to reach out to specific sectors to formulate sectoral codes
- Mechanism for feedback and information sharing across sector DPOs

- Sectors include
  - Government
  - Banking
  - Telecommunications
  - Business Process Outsourcing
  - Education
  - Insurance
  - Health

NATIONAL
PRIVACY
COMMISSION

The Data Protection Officer

Understanding NPC Advisory No. 17-01

General principles

NATIONAL PRIVACY COMMISSION

- The existence of a Data Protection Officer is the first indication of an entity's capacity to comply with the Data Privacy Act
- The DPO must be clothed with independence
- The DPO is bound by secrecy and confidentiality

Qualifications of a DPO

NATIONAL PRIVACY COMMISSION

- Should have specialized knowledge and demonstrable reliability
- Must be an expert in data privacy
- Must have sufficient understanding of the entity's data processing systems, security, and needs; must also know the field or industry of the entity and the entity's internal structure and policies

Qualifications of a DPO

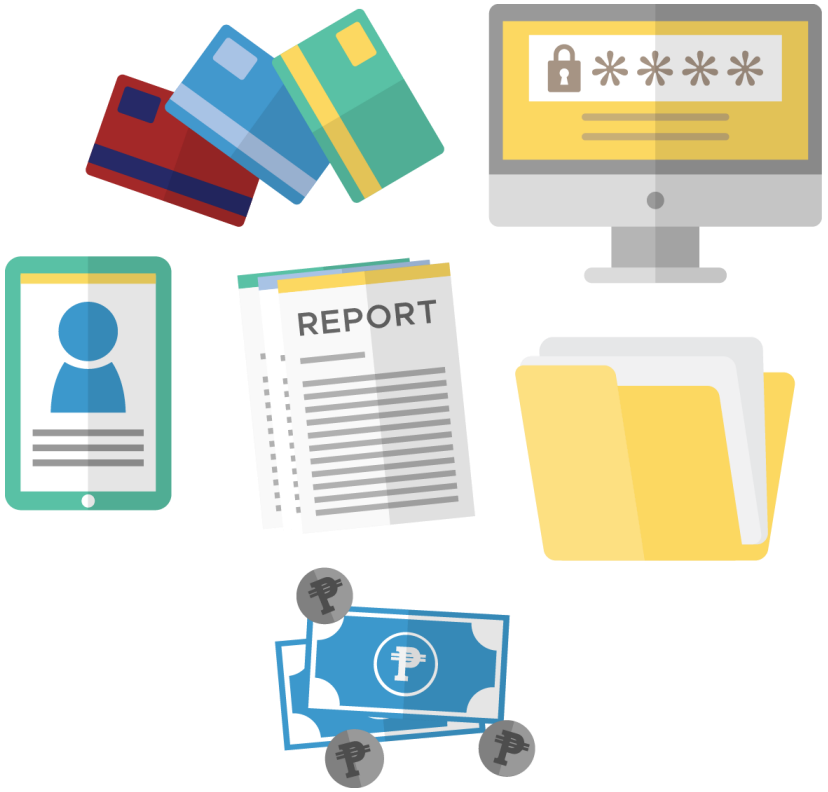
NATIONAL PRIVACY COMMISSION

- Preferably a regular or permanent employee, name replacement if necessary
- Contactual arrangements must be for at least two years
- No conflict of interest

Duties and Responsibilities

NATIONAL PRIVACY COMMISSION

- Monitor the performance of the entity in relation to the Data Privacy Act
- Ensure the conduct of a Privacy Impact Assessment
- Provide advice on the rights of data subjects
- Ensure proper compliance with breach management protocols
- Promote a culture of data privacy within the entity



Duties and Responsibilities

NATIONAL PRIVACY COMMISSION

- Advocate for the continuous development and review of privacy policies
- Serve as the contact person of the NPC within the organization
- Cooperate and seek advice from the NPC on data privacy issues

Monitoring performance and compliance

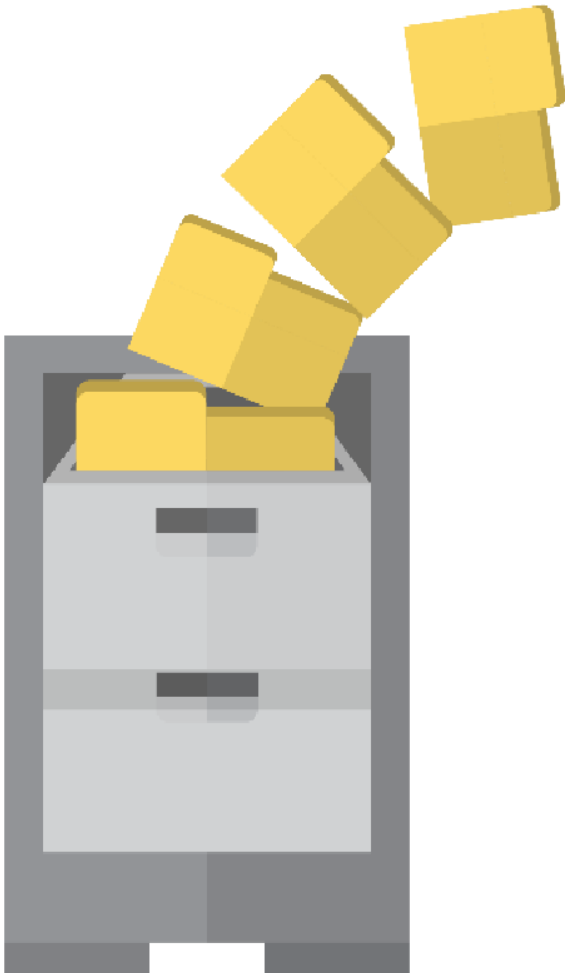
NATIONAL PRIVACY COMMISSION

- Collect information on the entity's processing activities
- Documenting the same
- Analyze and check compliance of the processes
- Inform and advise on issues, including data sharing agreements
- Ensure compliance with standards and certifications

Role of the entity

NATIONAL PRIVACY COMMISSION

- Involve the DPO at all stages
- Provide adequate resources and access
- Invite the DPO to middle management meetings
- Let the DPO take the lead in breaches



The DPO in holding companies

NATIONAL PRIVACY COMMISSION

- May appoint a group DPO, with the approval of the NPC.
- Lower officers are identified as Compliance Officer for Protection
- COPs have the same qualifications as the DPO

Outsourcing of functions

NATIONAL PRIVACY COMMISSION

- The DPO or COP may outsource particular functions
- The DOP or COP must still oversee the outsourced functions

Independence of the DPO

NATIONAL PRIVACY COMMISSION

- The DPO cannot be removed for performing his functions
- The opinion of the DPO carries great weight
- Extra duties that create conflict of interest is prohibited
- In case of dispute and recommendations are not followed, document reasons why

Publication of contact information

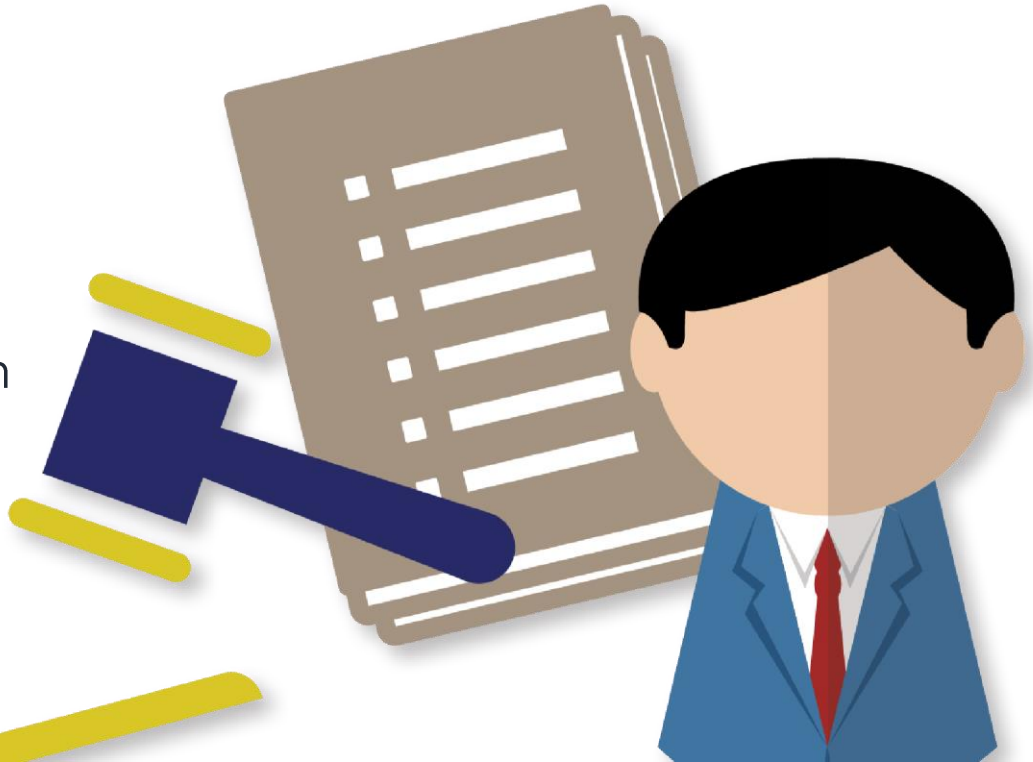
NATIONAL PRIVACY COMMISSION

- Contains name, dedicated phone and email, Physical Address
- Published in
  - Website
  - Privacy Notice
  - Privacy Policy
  - Privacy Manual

NATIONAL
PRIVACY
COMMISSION

Additional resources

privacy.gov.ph
facebook.com/privacy.gov.ph
twitter.com/privacyph



NATIONAL PRIVACY COMMISSION

End

francis.acero@privacy.gov.ph