NATIONAL PRIVACY COMMISSION

# All you need to know about the Data Privacy Act of 2012

**01 June 2017**
**Government CIO Summit**
**Las Casas Filipinas De Acuzar**

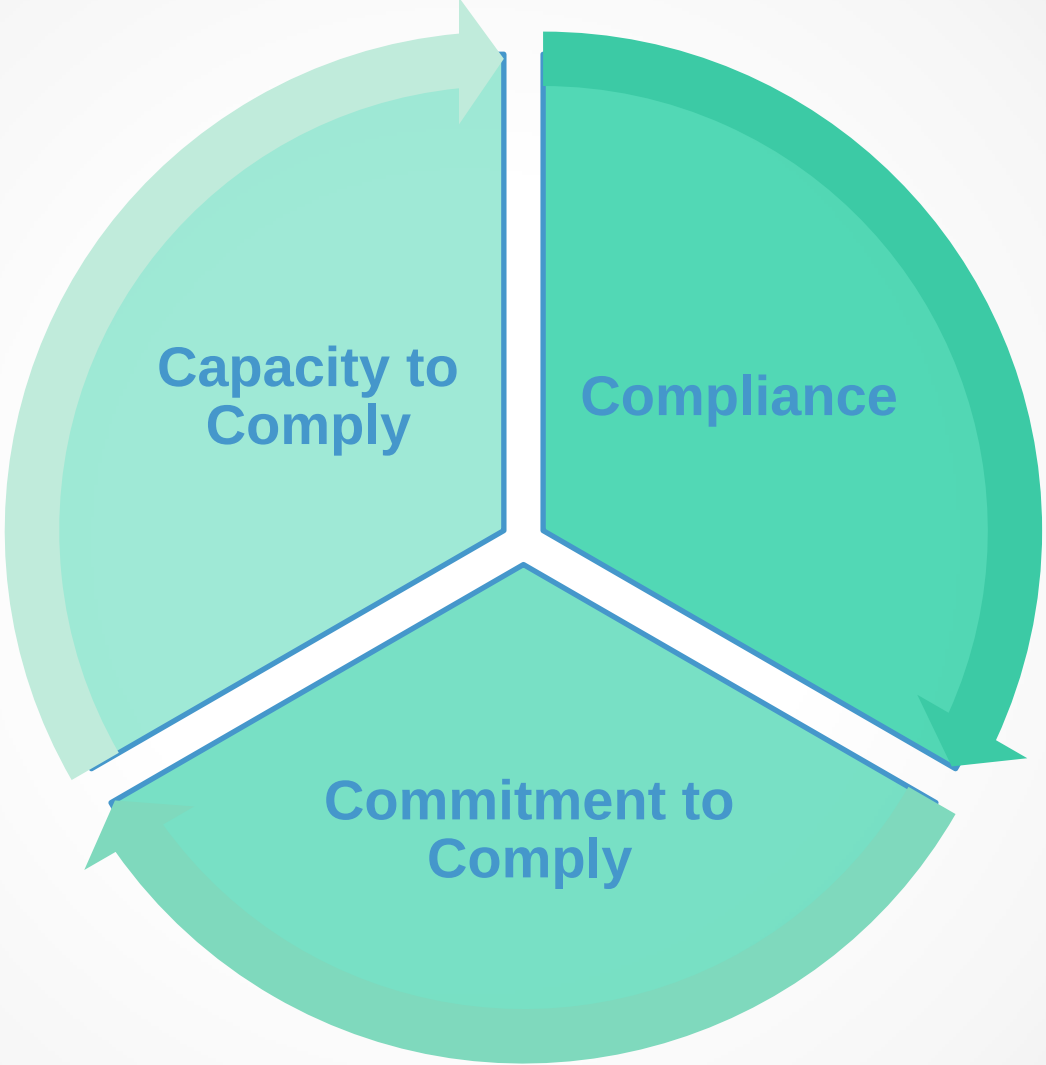
# Republic Act No. 10173

August 15, 2012

SECTION 1. *Short Title.* – This Act shall be known as the "Data Privacy Act of 2012".

SECTION. 2. *Declaration of Policy.* – It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth.

NATIONAL PRIVACY COMMISSION



# What can happen to you personally?


- **Sec. 22.** The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein…

- **Sec. 34.** Extent of Liability. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.

| Punishable Act | Jail Term | Fine (Pesos) |
|---|---|---|
| Access due to negligence | 1y to 3y – 3y to 6y | 500k to 4m |
| Unauthorized processing | 1y to 3y – 3y to 6y | 500k to 4m |
| Improper disposal | 6m to 2y – 3y to 6y | 100k to 1m |
| Unauthorized purposes | 18m to 5y – 2y to 7y | 500k to 2m |
| Intentional breach | 1y to 3y | 500k to 2m |
| Concealing breach | 18m to 5y | 500k to 1m |
| Malicious disclosure | 18m to 5y | 500k to 1m |
| Unauthorized disclosure | 1y to 3y – 3y to 5y | 500k to 2m |
| Combination of acts | 3y to 6y | 1m to 5m |

# Structure of RA 10173, the Data Privacy Act

Sections 1-6. Definitions and General Provisions

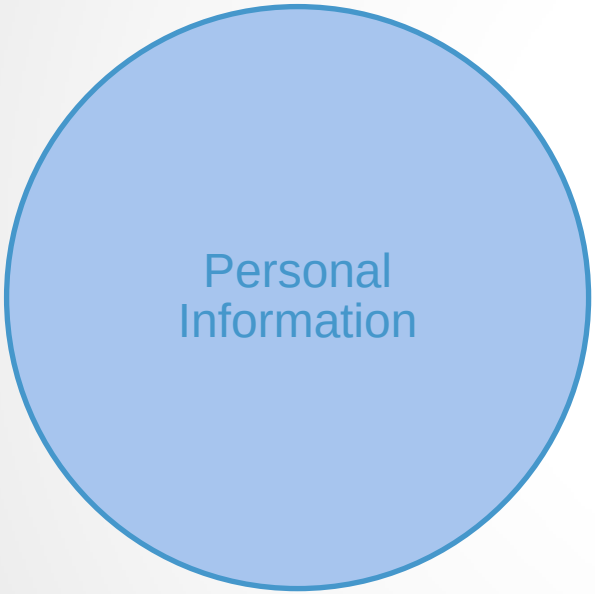
Sections 7-10. National Privacy Commission

Sections 11-21. Rights of Data Subjects, and Obligations of Personal Information Controllers and Processors

Section 22-24. Provisions Specific to Government

Section 25-37. Penalties

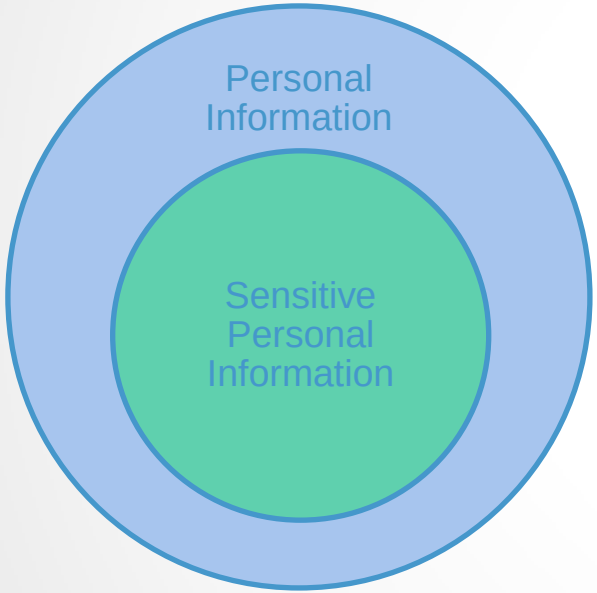
# Definitions




*Personal information* 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.

*– RA. 10173, Section 3.g*

# Definitions




*Sensitive personal information* 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.

*– RA. 10173, Section 3.l*

# Key Definitions

PIC

**“Personal Information Controllers”** those who decide what data is collected and how it is processed (example: Bank X, Hospital Y).

PIP

**“Personal Information Processors”** those who process data as instructed by the controllers (example: shared services, IT vendor, external lab).


# The Obligations which must be complied with by PICs and PIPs

Data Privacy Act of 2012

IRRs
(promulgated 2016)

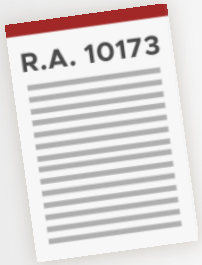
**2016 Series (issued)**

- Circular 16-01 — Gov't Agencies
- Circular 16-02 — Data Sharing
- Circular 16-03 — Breach Mgmt
- Circular 16-04 — Rules Procedure

**2017 Series**

- *Advisory 17-01 — DPO Guidelines*
- *Draft Circular — DOH-Regulated*
- *Draft Circular — BSP-Supervised*

# How should you comply?
## R.A. 10173, Data Privacy Act of 2012




- SEC. 20 (a) 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.

- Sectors can craft their own **“privacy codes”** to address relevant industry issues and practices. For government, Circulars 16-01 and 16-02 are part of our “sectoral code”.

NATIONAL PRIVACY COMMISSION

# Obligations of PICs/PIPs

- Uphold the rights of data subjects
- Appoint a DPO/Compliance Officer
- Process according to Privacy Principles
- Establish Data Protection framework
- Setup Breach Reporting Procedure
- Register systems with the NPC

# #1: Uphold the rights of data subjects

Legal Basis: Sec. 16-18 and 38, IRR 17-24, 34-37

## What compliance looks like

- ❑ Data subjects are apprised of their rights through a privacy notice
- ❑ Data subjects know who to complain to if their rights are violated
- ❑ Complaints are acted upon quickly

## What negligence looks like

- ❑ No privacy notice when data is collected
- ❑ No contact details on how to lodge a complaint
- ❑ Complaints take a long time to be remedied

NATIONAL PRIVACY COMMISSION

# #2: Appoint a DPO (Data Protection Officer)

Legal Basis: Sec. 21, IRR 50, Circ. 16-01, Advisory 17-01

**Sec. 21 (b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act.**

NATIONAL PRIVACY COMMISSION

# #2: Appoint a DPO (Data Protection Officer)

Legal Basis: Sec. 21, IRR 50, Circ. 16-01, Advisory 17-01

## What compliance looks like

- ❑ Notarized appointment or designation of a DPO, filed with the NPC
- ❑ Evidence of actions taken on basis of DPO recommendations
- ❑ Contact details on website (if any)
- ❑ Continuing education program

## What negligence looks like

- ❑ No DPO
- ❑ Lack of interaction between DPO and top management, between DPO and functional units
- ❑ Inaction on complaints from data subjects
- ❑ Non-reporting to NPC

NATIONAL PRIVACY COMMISSION

# #3: Data Processing adheres to Transparency, Legitimate Purpose, and Proportionality

Legal Basis: Sec. 11-15, IRR 21-23 and 43-45, Circ. 16-01 and 16-02

## What compliance looks like

- ❑ Privacy policies cascaded throughout the organization and updated as needed
- ❑ Data handlers have security clearance and privacy training
- ❑ Privacy notice where appropriate, e.g. on website
- ❑ Data sharing agreements in place
- ❑ Privacy impact assessments conducted and up-to-date
- ❑ Service providers in compliance

## What negligence looks like

- ❑ Privacy policy sits on shelf
- ❑ No security clearance or privacy training for data handlers
- ❑ No privacy notice when collecting personal data
- ❑ Overcollection
- ❑ Data sharing without agreements
- ❑ No privacy impact assessments
- ❑ No compliance obligations for service providers

NATIONAL PRIVACY COMMISSION

# Principles

**“Transparency” –** no surprises in how the data collected is being processed

**“Legitimate purpose” –** required by law and not contrary to public morals

**“Proportionality” –** collect only what’s needed and commensurate to the benefits

NATIONAL PRIVACY COMMISSION

# #4: Maintain Confidentiality, Integrity, Availability

Legal Basis: Sec. 20.a-e, Sec. 22 and 24, IRR 25-29, Circ. 16-01

**Sec. 20 (c)** "The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation."

***How will you know what are "the risks represented by the processing"?***

NATIONAL PRIVACY COMMISSION

# #4: Maintain Confidentiality, Integrity, Availability

Legal Basis: Sec. 20.a-e, Sec. 22 and 24, IRR 25-29, Circ. 16-01

## What compliance looks like

- ❑ Data protection risks identified, and the appropriate up-to-date controls are in place to manage these risks
- ❑ Data protection policies cascaded throughout the org'n and updated as needed
- ❑ Frequent monitoring and vulnerability scanning
- ❑ Regular security and business continuity drills are conducted
- ❑ Service providers in compliance

## What negligence looks like

- ❑ Generic controls in place
- ❑ Controls not updated for new risks/threats
- ❑ Controls are not complied with
- ❑ Lax cyber-hygiene practices
- ❑ No compliance obligations for service providers
- ❑ No periodic drills or monitoring
- ❑ No venue for data subjects to access or correct/rectify their own data

NATIONAL PRIVACY COMMISSION

# Circular 16-01, Sections 7 to 13 Processing of Personal Data

## "Owned" Data Center

- Covered as PIC
- Subject to NPC Audit (Sec. 11)
- AES-256 Encrypted (Sec. 8)
- Access control system (Sec. 9)
- Archives are also covered (Sec. 13)
- ISO 27001/27002

## "Non-owned" Data Center

- Covered as PIP (sec. 10)
- Subject to NPC Audit (Sec. 11)
- ISO 27018 (Sec. 12)
- AES-256 Encrypted (Sec. 8)
- Archives are also covered (Sec. 13)
- Contract subject to review (Sec. 7)
- If data is stored outside the country, geographic location must be specified in contract (IRR, Sec. 44.a)

NATIONAL PRIVACY COMMISSION

# ISO 27001 vs 27018 Benefits

## 27001 – your data is stored in your own data center

- You have a clear picture of what your information security risks are
- You can identify a set of controls to manage your risks
- You can monitor the ongoing implementation and deployment of the selected controls

## 27018 – your data is stored in someone else's data center

- You have control over which country your data will be stored in
- Your data won't be used for marketing or advertising without your consent
- You will be notified of legal requests for data disclosure

NATIONAL PRIVACY COMMISSION

# Other recommendations

A. Limit access to data to authorized users, devices, and programs *(Circular 16-01, Sections 14 to 21)*
B. Apply similar security and access controls to non-digitized files/media *(Circular 16-01, Section 22)*
C. Use secure channels when transferring personal data *(Circular 16-01, Sections 24 to 29)*
D. Observe proper procedures for disposal/archiving of personal data *(Circular 16-01, Sections 30 to 32)*

# #5: Report Breach within 72 hours

Legal Basis: Sec. 20.f and 30, IRR 38-42 and 57, Circ. 16-03

**IRR Sec. 38 (a)** The Commission and affected data subjects shall be notified by the PIC within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred.

NATIONAL PRIVACY COMMISSION

# #5: Report Breach within 72 hours

Legal Basis: Sec. 20.f and 30, IRR 38-42 and 57, Circ. 16-03

## What compliance looks like

- ❑ Formation of a data breach response team with clearly defined roles and responsibilities
- ❑ Clearly defined and up-to-date incident response procedure that covers assessment, mitigation, notification and recovery actions
- ❑ Regular breach drills are conducted
- ❑ Service providers in compliance

## What negligence looks like

- ❑ No response team or procedures
- ❑ No drills
- ❑ No compliance obligations for service providers
- ❑ No post-breach reports
- ❑ No notification within 72 hours (an act punishable by 18 months to 5 years of imprisonment and and a fine of 500,000 to 1,000,000 pesos)

NATIONAL PRIVACY COMMISSION

# Finally: Register with the NPC

## Legal Basis: Sec. 24, IRR 33 and 46-49

### What compliance looks like

- ❑ Registration with the NPC is up-to-date and contains all necessary compliance documentation
- ❑ Registration includes all automated processing operations that would have legal effect on the data subject
- ❑ Annual report summarizing documented security incidents and personal data breaches
- ❑ Service providers in compliance

### What negligence looks like

- ❑ No registration
- ❑ Out-of-date registration
- ❑ No compliance obligations for service providers

NATIONAL PRIVACY COMMISSION

NATIONAL PRIVACY COMMISSION

**Designating a DPO is the first essential step towards compliance. You cannot register your systems with the NPC unless you have a DPO. You cannot report your compliance activities unless you go through your DPO.**

# When should you comply?


**Yesterday.** Obligations in the DPA and the IRR.

**September 2017.** Additional Requirements in the IRR: Registration of Data Processing Systems and Automated Processing, 72-hour Breach Notification, Annual Incident Reporting

**October 2017. S**ecurity requirements in Circular 16-01 for Government Agencies.

NATIONAL PRIVACY COMMISSION

# Thank you!

PRIVACY.GOV.PH

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

NATIONAL
PRIVACY
COMMISSION