# Understanding the Regulatory and Investigative Powers of the National Privacy Commission

**Francis Euston R. Acero**
Complaints and Investigations Division

# What do I expect to learn today?

Expectation-setting

# Objectives

***Why do we need for regulatory oversight in data protection?*** Learn the necessity for data privacy and protection oversight.

***How does the National Privacy Commission treat private information controllers and processors?*** Find how the NPC approaches compliance with the provisions of the Data Privacy Act of 2012 and what the NPC looks for in its investigations.

***How does the NPC handle data breaches and complaints?*** Get a basic idea of how the NPC handles issues brought to its attention.

# What makes an excellent regulator?

Selections from the Volker Institute at the Penn Program on Regulation Best-in-Class Regulator Initiative

# Mission

***The excellent regulator understands its mission and sets goals to achieve its mission.*** The different parts of the organization must understand how each part contributes to the larger goal, and each goal to the larger mission.

The understanding of this mission must be flexible enough to adapt to changing times.

The NPC's core regulatory functions are handled by the Data Security and Compliance Office, the Legal and Enforcement Office, and the Privacy Policy Office.

# Funding

***Adequate funding ensures that the regulator avoids risk buildup.***

"The best rules will fall short without effective supervision and enforcement." – U.S. Treasury Secretary Jack Lew

It is important for the regulator to be confident in the exercise of its jurisdictional power.

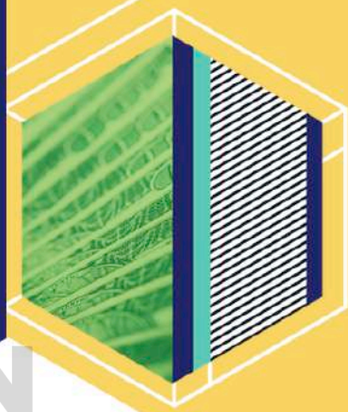
Currently, the NPC has funding of ₱160 million; more is expected in the coming years.

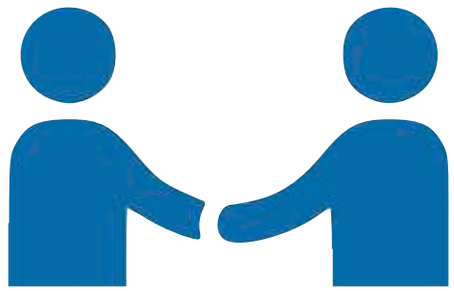
# Understanding

***The regulator must understand the risks and conditions affecting its mission; the industry it regulates; its own risk profile; and a means by which it can deploy with maximum impact.***

Misallocating resources and an over-reliance on checklist methodologies leaves gaps in supervision and regulation; regulators are lulled into complacency.

Our DPO series allows the NPC to understand our regulated industries better.





# Influence

***The ability to influence outcomes across regulated industries comes from the regulator's unique horizontal perspective.***

The NPC's Data Security and Compliance Office has the mandate of looking horizontally across regulated industries, to encourage the adoption of what works best.

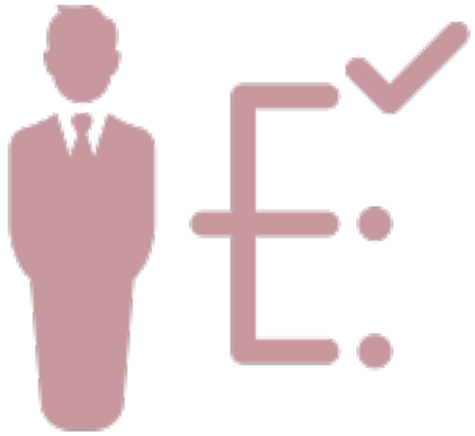
# Communicate

***Excellent regulatory bodies regularly communicate with the public on why they exist.***

Awareness that violators get caught raises the sense of fairness in those who comply with the law.

# How does the NPC treat controllers and processors?

The NPC's mandate and function under the Data Privacy Act of 2012



# Regulator

To administer and implement the provisions of this Act, and ***to monitor and*** **ensure compliance of the country with international standards set for data protection**, there is hereby created an independent body to be known as the National Privacy Commission. (7)

Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner ***mindful of the rights and interests of the individual about whom personal information is processed***. (38)

# Coordinator

***Coordinate with other government agencies and the private sector*** on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country. (7f)

***Review, approve, reject or require modification of privacy codes*** voluntarily adhered to by personal information controllers. (7j)

# Watchdog

Ensure ***compliance*** of personal information controllers. (7a)

Compel or petition any entity, government agency or instrumentality to ***abide by its orders or take action on a matter affecting data privacy***. (7d)

# *Investigator*

Receive ***complaints, institute investigations,*** facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report.

# Adjudicator

Receive *complaints, institute investigations,* ***facilitate or enable settlement of complaints through the use of alternative dispute resolution*** processes, adjudicate, ***award indemnity on matters affecting any personal information***, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report.

# How does the NPC fulfill its mandate?

Processes and front-line services at the National Privacy Commission

# Complaints

The Complaints and Investigations Division conducts the initial phase of the complaints resolution procedure as outlined in NPC Circular No. 16-04.

The NPC has mandatory discovery processes to speed up dispute resolution.

Circular No. 16-04 also contains exhaustion provisions.

Parties are afforded an opportunity to present their sides before coming to a decision.

# Investigations

The Complaints and Investigations Division spearheads the fact-finding investigations of the National Privacy Commission.

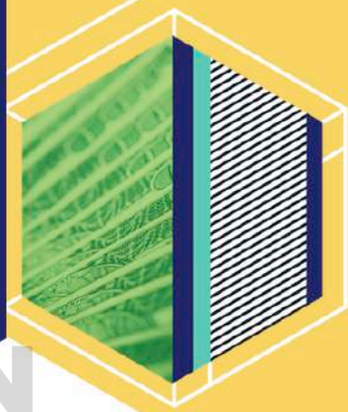
The CID has received training from the FBI and from local law enforcement on digital forensics and digital artifact retrieval and documentation.

# Standards

The Commission has set standards for data protection and privacy for government offices through NPC Circular No. 16-01.

**Highlights**:

- Requires the appointment of a DPO
- Requires the regular conduct of a privacy impact assessment, review of the control framework, and breach management procedure.
- Requires 256-bit encryption for standing and traffic data.
- Requires remote wipe for BYOD policies.
- Requires full disk encryption for laptops, portable media storage.



# Standards

These DPO forums are done as part of the push toward the adoption of industry-specific data privacy codes.

The Data Security and Compliance Office and the Privacy Policy Office are lead offices in crafting these policies.



# What does the NPC look out for?

Red flags in regulatory and investigative frameworks

# Regulatory

**Red flags include**:

- Absence of clear lines of responsibility and/or directly responsible officers on data privacy and protection issues.
- Absence of privacy management and breach management policies.
- Absence of technical and physical safeguards in entire data life cycle.
- Little to no organizational awareness on data protection and privacy issues, especially from the top.

# Investigative

**Red flags include**:

- Confirmed reports of data proliferating in the wild.
- Incriminatory results from other parallel investigations from other law enforcement agencies.
- Willfully ignoring or neglecting to address known vulnerabilities and issues spotted by other actors.

# Where can we get more information?

Contact us!

**PRIVACY.GOV.PH**

facebook.com/privacy.gov.ph

twitter.com/privacyph

info@privacy.gov.ph