NATIONAL PRIVACY COMMISSION

How to comply with the Data Privacy Act of 2012

Dondi Mapa
Deputy Privacy Commissioner
for Data Processing Systems

Which is more valuable?

Data

Money

ANDY GREENBERG SECURITY 04.04.17 10:52 AM

HOW HACKERS HIJACKED A BANK'S ENTIRE ONLINE OPERATION

GETTY IMAGES

WorldViews • Analysis

The era of cyber-disaster may finally be here

By Adam Taylor May 15 at 1:00 AM

On Friday, the world was hit by one of the biggest cyberattacks in recent history.

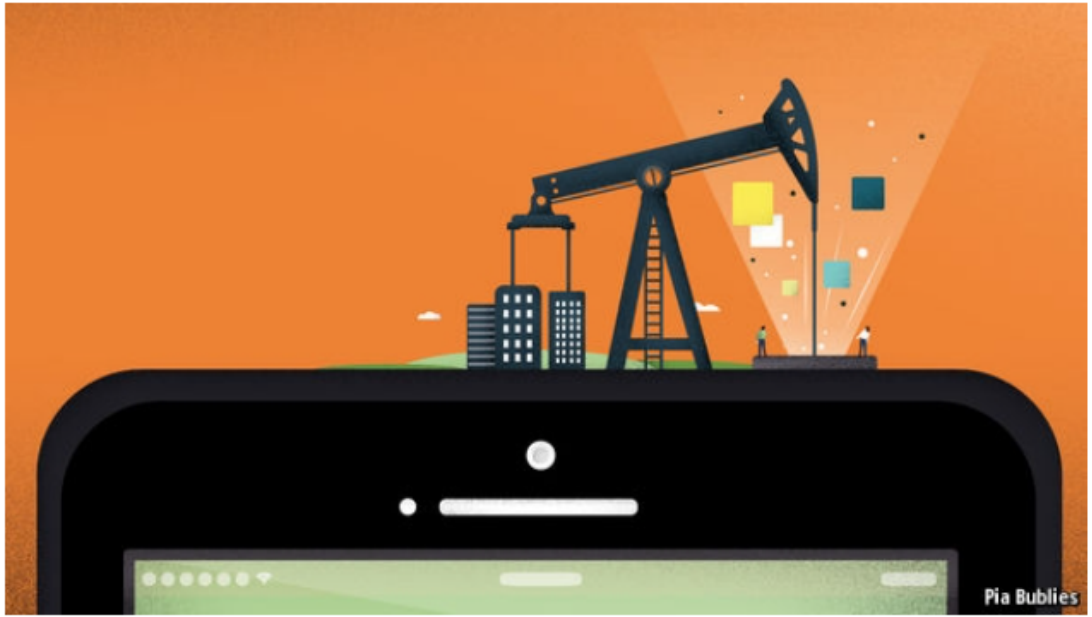
economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy

The Economist | Topics | Print edition | More

Fuel of the future

Data is giving rise to a new economy

How is it shaping up?



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

So... you didn't comply with the Data Privacy Act.

What's the worst that could happen?

SECTIONS Tuesday, January 3, 2017 INQUIRER.NET

55M at risk in 'Comeleak'

By: Tina G. Santos - Reporter / @santostinaINQ Philippine Daily Inquirer / 12:44 AM April 23, 2016

DECEPTIVE CALM The Comelec office at Palacio del Gobernador in Intramuros,Manila, after office hours. The Comelec says the hacking of its website will not compromise the integrity of national elections on May 9. EDWIN BACASMAS

Precinct Finder Database (55m + 17m)

- Vulnerable to targeted marketing
- Vulnerable to identity theft
- Increased cost to verify identity
- Higher risk of re-identification
- Higher cost of de-identification

Post Finder Database (1.3m)

- Highly vulnerable to identity theft
- Possible risk of blacklist/no-fly list
- Cost of passport renewals

Gun Ban Exemptions Database (900k)

- Increased risk of physical targeting

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

NATIONAL PRIVACY COMMISSION

Structure of RA 10173, the Data Privacy Act

Sections 1-6. Definitions and General Provisions

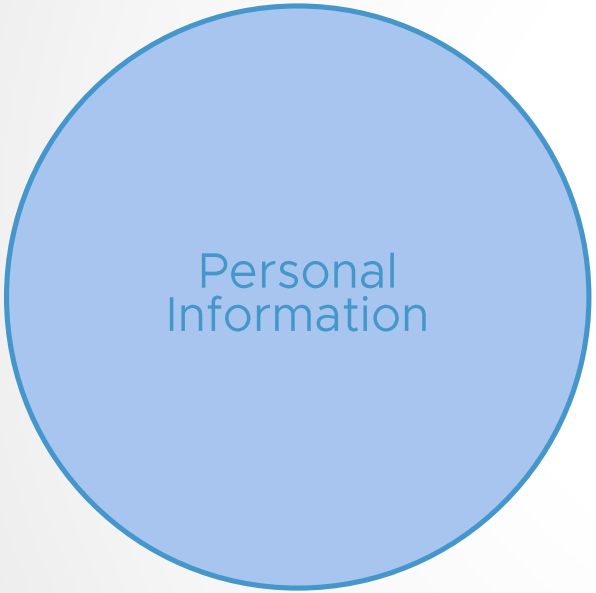
Sections 7-10. National Privacy Commission

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

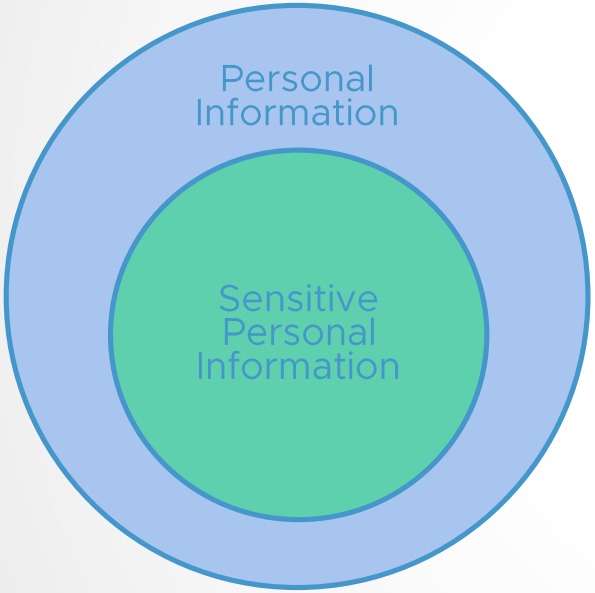
Definitions



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

NATIONAL PRIVACY COMMISSION

My Australian friend's "bank security question"

Q: What was the name of your pet dog in Adelaide?
A: Neptune

Key Definitions

NATIONAL PRIVACY COMMISSION

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).

Are there exemptions?

- **RA 10173, Section 4. Special Cases.** The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:

- **f.** Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510 otherwise known as the Credit Information System Act (CISA), and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws;

- The information is exempt, but you are not...

- Consider an example where you are processing an application for a bank loan. Is consent required for reporting such transaction to the AMLC or CIC? NO

- HOWEVER,
  - if there is a breach of Confidentiality
    - You improperly disclose the data
  - if there is a breach of Integrity
    - You allow the data to be altered
  - if there is a breach of Availability
    - You fail to ensure business continuity

- YOU can become the subject of a data privacy complaint.

What happens if you don't comply?

Sec. 7. Functions of the National Privacy Commission…

(b) 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…

(c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;

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

(i) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act;

NATIONAL PRIVACY COMMISSION

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

NATIONAL PRIVACY COMMISSION

Our Rights as Data Subjects

- ✓ Right to be informed
- ✓ Right to object
- ✓ Right to access
- ✓ Right to correct/rectify
- ✓ Right to block/remove
- ✓ Right to data portability
- ✓ Right to file a complaint
- ✓ Right to be indemnified

Keep calm and complain

(See procedure in NPC Circular 16-04)

- Was personal data collected from you in a manner that was not transparent, legitimate or proportional?
- Was your personal data used without your consent to make an automated decision about you that has legal effect?
- Was your personal data mishandled in terms of confidentiality and/or availability?
- Did someone tamper with your personal data without your knowledge?
- Was your personal data improperly disposed of, maliciously disclosed, or used in an unauthorized manner?
- Did you suffer harm as a result of a personal data breach?

NATIONAL PRIVACY COMMISSION

NATIONAL PRIVACY COMMISSION

Republic Act No. 10173

August 15, 2012

SEC. 17. Transmissibility of Rights of the Data Subject. – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

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

The Obligations which must be complied with by PICs and PIPs

Data Privacy Act of 2012

IRRs (promulgated 2016)

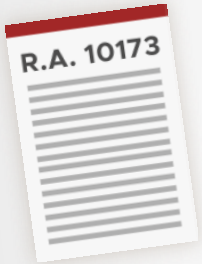
2016 Series (issued)

- 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.

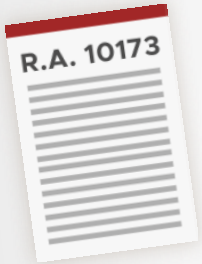
- Sectors can craft their own "privacy codes" to address relevant industry issues and practices. These codes can be submitted to the NPC for review/comment.

NATIONAL PRIVACY COMMISSION

Sectoral Codes

- SEC. 7.j The NPC can Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers:
- *Provided,* That the privacy codes shall adhere to the underlying data privacy principles embodied in this Act:
- *Provided, further,* That such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller.
- For this purpose, the Commission shall consult with relevant regulatory agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law:
- *Provided, finally.* That the Commission may review such privacy codes and require changes thereto for purposes of complying with this Act;

Sectoral Code for Banking sector can address the following common concerns:



- Who can be appointed DPO?
- When can data be stored in the cloud?
- What encryption standard should be used?
- What standards to use when reporting a breach?
- What kind of data sharing agreement is needed for AMLC and CIC?

Data Privacy Act (RA 10173) Compliance Checklist

Compliance with Sec. 16-18 and 38 of the DPA and Sections 17-24, 34-37 of the IRR and Circular 16-04

- ☐ 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 (within 30 days)

Compliance with Sec. 21 of the DPA, Section 50 of the 50, Circular 16-01, and Advisory 17-01

- ☐ Notarized appointment or designation of a DPO/COP, filed with the NPC
- ☐ Evidence that actions have been taken on the basis of DPO/COP recommendations
- ☐ Contact details on website (if any)
- ☐ Continuing education program for the DPO/COP

Compliance with Sec. 11-15 of the DPA, Sections 21-23 and 43-45 of the IRR, Circulars 16-01 and 16-02

- ☐ Personal data is processed under conditions specified in Sections 12 and 13 of the DPA
- ☐ 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, in offices
- ☐ Data sharing agreements in place
- ☐ Privacy impact assessments conducted and up-to-date
- ☐ Service providers agree to honor their compliance obligations

Compliance with Sec. 20.a-e, 22 and 24 of the DPA, Sections 25-29 of the IRR, Circular 16-01

- ☐ Data subjects are provided a venue to correct/rectify their data
- ☐ Data protection risks have been identified and documented
- ☐ Appropriate and up-to-date controls are in place to manage these risks (e.g ISO:IEC 27002)
- ☐ Data protection policies are cascaded throughout the organization and updated as needed
- ☐ Vulnerability scanning is conducted at least once a year
- ☐ Business continuity drills are conducted at least once a year
- ☐ Service providers agree to honor their compliance obligations
- ☐ If data is stored in the cloud, provider is ISO:IEC 27018 compliant
- ☐ For data stored outside the country, privacy jurisdiction has been defined
- ☐ Digitized personal data is encrypted using 256-bit AES

Compliance with Sec. 20.f and 30 of the DPA, Sections 38-42 and 57 of the IRR, Circular 16-03

- ☐ Formation of a data breach response team with clearly defined roles and responsibilities
- ☐ Clearly defined and up-to-date incident response procedure
- ☐ Breach drills are conducted at least once a year
- ☐ Service providers agree to honor their compliance obligations

Compliance with Sec. 24 of the DPA, and Sections 33 and 46-49 of the IRR

- ☐ Registration with the NPC is up-to-date and contains all necessary compliance documentation
- ☐ Registration of all automated processing operations that have legal effect on the data subject
- ☐ Annual report summarizing documented security incidents and personal data breaches
- ☐ Service providers agree to honor their compliance obligations

#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

#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

#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.

Checklist for Data Protection Officer (DPO)

Within 30 days:

- ☐ Draw up your TOR. Be sure to get an assurance that you shall be reimbursed in case of litigation related to the Data Privacy Act.
- ☐ If your organization is considered medium- or high-risk, you may want to consider forming a data protection task force or committee, or at the least, having an assistant DPO.
- ☐ Register your appointment/designation with the NPC, likewise, update organization's website to reflect such.
- ☐ Join an existing network of privacy professionals, such as the IAPP (International Association of Privacy Professionals). Or organize one yourself, perhaps your industry association could have a special interest group for DPOs.
- ☐ Reach out to your counterpart in a similar organization in Europe, Canada, Australia or the US. He or she can coach you about the role, and can share their best practices.
- ☐ Send out an RFQ for an external consultant to do an IT Security audit to discover what are your organization's "pre-existing conditions".
- ☐ Send out an RFQ for a software application to assist you in monitoring compliance of the organization. These tools should include features such as workflow management, and document management.
- ☐ Obtain an organizational inventory of processes that handle personal data, including the list of process owners.

Within 90 days:

- ☐ Acquire and deploy a software application to assist you in monitoring compliance of the organization. These tools should include features such as workflow management, and document management.
- ☐ Develop your own plan for continuing education and consider working towards a certification such as IAPP's CIPT and CIPM certifications.
- ☐ Schedule workshops with all process owners to do a Privacy Impact Assessment (PIA) of the process/es which they own.
- ☐ Use the results of the PIAs to begin drawing up your organization's control framework for privacy and data protection.
- ☐ Select an external consultant to conduct an IT Security audit, and initiate such audit.
- ☐ Establish a breach management framework for the organization.

Within 180 days:

- ☐ Review results of IT Security audit with top management.
- ☐ Ensure that all those who are handling personal data have been issued a security clearance by the head of organization.
- ☐ With the help of HR, Legal, IT, and Security, begin drafting your organization's privacy and data protection policies. If your organization handles personal data for more than 1,000 individuals, NPC recommends the use of the ISO/IEC 27002 control set as the minimum standard to assess any gaps in your control framework.
- ☐ Select a governance framework that will help you strategize and orchestrate the implementation of the organization's privacy programs. There are several available, and you may want to start with a simple one. Within 12 to 18 months, you can then assess whether you need to evolve to a more advanced framework. This is consistent with an approach of continuous assessment and development, taking into account inputs from top management and the process owners.
- ☐ Conduct breach management drill/s, prioritizing those processes with the highest privacy risk.

Checklist for CEO/Head of Agency

Within 30 days:

- ☐ Designate a DPO and ensure he/she has access to top management. This can be done either through direct reporting on the organizational structure, or through membership in the executive committee. It is important that your DPO is up-to-date on the strategic issues and change drivers that are impacting your organization.
- ☐ Send out an announcement to the organization that the DPO is the "privacy champion" and the point of contact within the organization for anything related to compliance with the Data Privacy Act.
- ☐ Make compliance to the Data Privacy Act part of the performance bonus criteria of divisions of the organization who are involved with privacy compliance, such as HR, Legal, IT, Security, etc.
- ☐ If your organization is considered medium- or high-risk in terms of privacy impact, consider forming a data protection task force or committee, and keep in mind that an organization can have more than one DPO. This allows DPO skills, expertise and tasks to be distributed across the entire DPO team. However, it should be clear who holds overall responsibility and accountability.
- ☐ Assign the head of Legal to ensure that all service provider contracts, job orders, etc. are compliant. For example, all service providers must also have their own DPO.
- ☐ Assign the head of Legal to ensure that all external sharing of data meets the required guidelines of the NPC.

Within 90 days:

- ☐ Support your DPO in scheduling PIA workshops, and in ensuring that the process owner(s) take full ownership of the PIA outputs.
- ☐ Ask DPO for the calendar of training and education events related to privacy management.
- ☐ Drive the urgency within the organization to comply with the Data Privacy Act.
- ☐ Assign head of HR to issue security clearances to all organization personnel and consultants who process personal data.

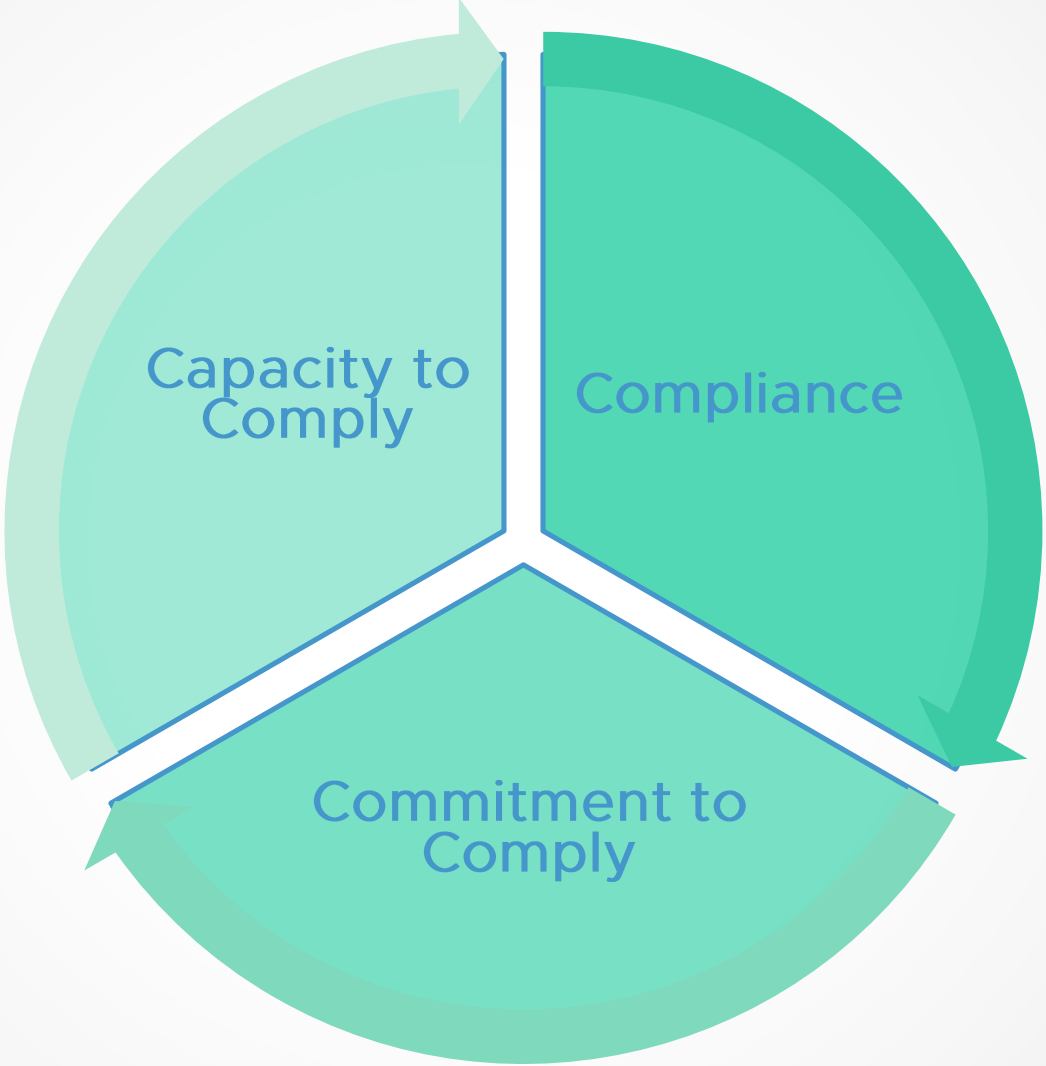
Within 180 days:

- ☐ Ensure that breach drills are being conducted on a regular basis.
- ☐ Ask DPO for results of the IT Security audit and the Privacy Impact Assessments.

For questions or comments on this checklist, please contact info@privacy.gov.ph

NATIONAL PRIVACY COMMISSION


In today's data-driven economy, privacy has become the proxy for trust: if you allow my privacy to be breached, you lose my trust, and if you lose my trust, you lose my business.
Dondi Mapa
Deputy Privacy Commissioner
Republic of the Philippines


Capacity to Comply
Compliance
Commitment to Comply


"The difference between compliance to the Data Privacy Act and accountability to the Filipino people and their data privacy rights, is the difference between doing what is required and doing all that is necessary."
Dondi Mapa
Deputy Privacy Commissioner for Data Processing Systems
NATIONAL PRIVACY COMMISSION

Thank you!

dmapa@privacy.gov.ph
0920-920-1071

PRIVACY.GOV.PH

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

NATIONAL
PRIVACY
COMMISSION