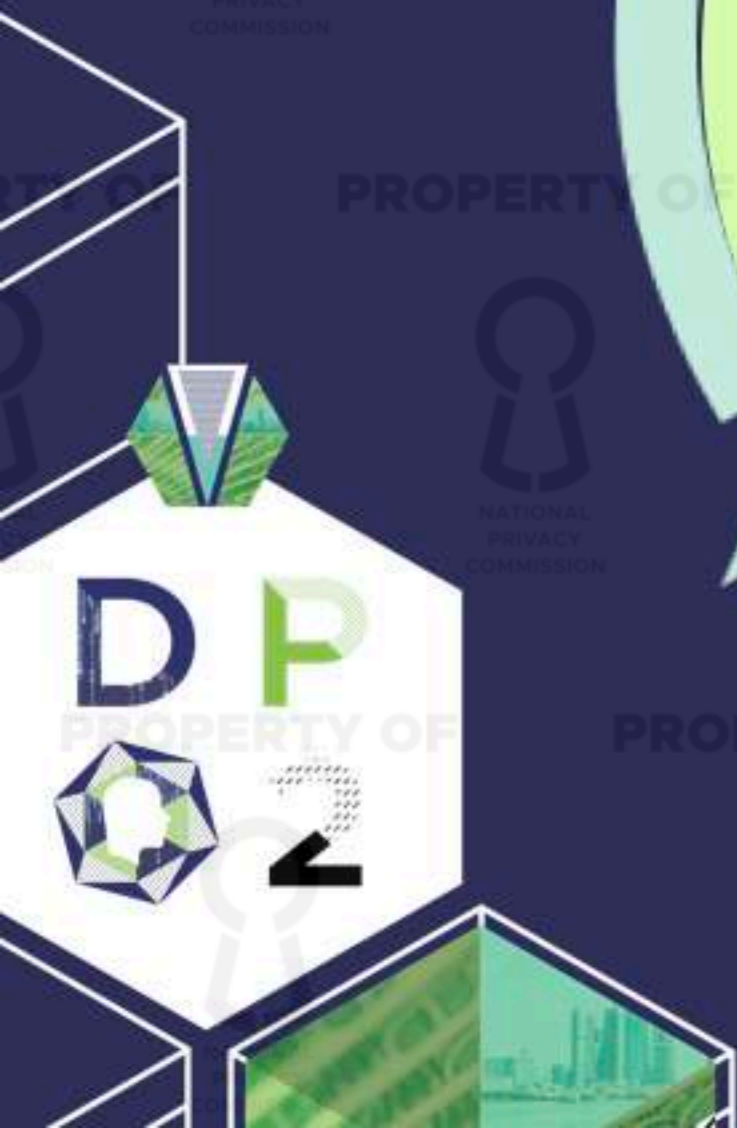


# *How to Comply with the Data Privacy Act of 2012*

**Dondi Mapa**

Deputy Privacy Commissioner  
for Data Processing Systems



***What can  
happen to  
you  
personally?***

**DP**  
2



## **Section 22**

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

## **Section 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**

**1 year to 3 years; 3 years to 6 years**

**500K to 4M**

**Unauthorized Processing**

**1 year to 3 years; 3 years to 6 years**

**500K to 4M**

**Improper Disposal**

**6 months to 2 years; 3 years to 6 years**

**100K to 1M**

**Unauthorized Purposes**

**18 months to 5 years; 2 years to 7 years**

**500K to 2M**

**Intentional Breach**

**1 year to 3 years**

**500K to 2M**

**Concealing Breach**

**18 months to 5 years**

**500K to 1M**

**Malicious Disclosure**

**18 months to 5 years**

**500K to 1M**

**Unauthorized Disclosure**

**1 year to 3 years; 3 years to 5 years**

**500K to 2M**

**Combination of Acts**

**3 years to 7 years**

**1M to 5M**



# ***Are there exemptions?***



# **RA 10173, Section 4. Scope**



The Act does not apply to the following:

**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 inadvertently 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 data privacy complaint.**



# ***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  
Government  
Agencies

Circular  
16-02  
Data Sharing

Circular  
16-03  
Breach  
Management

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.

# 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?

What data can 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?

Can depositors be asked to “waive all privacy rights”?

# ***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***

**DPD**  


## 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 IRR, 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



2

# ***Appoint a DPO***

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.

# Appoint a DPO

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

# What does a DPO do?

- a. monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies.
- b. ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
- c. advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
- d. ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
- e. inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;
- f. advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;
- g. serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
- h. cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
- i. perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

**What  
does  
a COP  
do?**

**See NPC Advisory 2017-01, pp. 6-7**

## **DPO: Data Protection Officer**

## **COP: Compliance Officer for Privacy**

- For COP, NPC will approve if: “supervised” by a DPO, low to medium risk, must show how “binding” applies (pp. 4-5)
- Must be an employee of the PIC or PIP (p. 5)
- No conflict of interest – cannot also be a data or process owner (p. 6)
- The functions of a DPO or COP **may be subcontracted or outsourced** to a third-party service provider (p. 8)
- The PIC or PIP should not directly or indirectly penalize or dismiss the DPO or COP for performing his or her tasks (p. 8)
- The PIC or PIP **should follow the advice** of the DPO or explain and document why it did not (p. 9)

# ***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

# 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”?*

# 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

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.



# 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 a fine of 500,000 to 1,000,000 pesos)

# Register systems 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

***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](mailto:info@privacy.gov.ph)



***damp@privacy.gov.ph***

0920 920 10 71

**PRIVACY.GOV.PH**

[facebook.com/privacy.gov.ph](https://facebook.com/privacy.gov.ph)

[twitter.com/privacyph](https://twitter.com/privacyph)

[info@privacy.gov.ph](mailto:info@privacy.gov.ph)