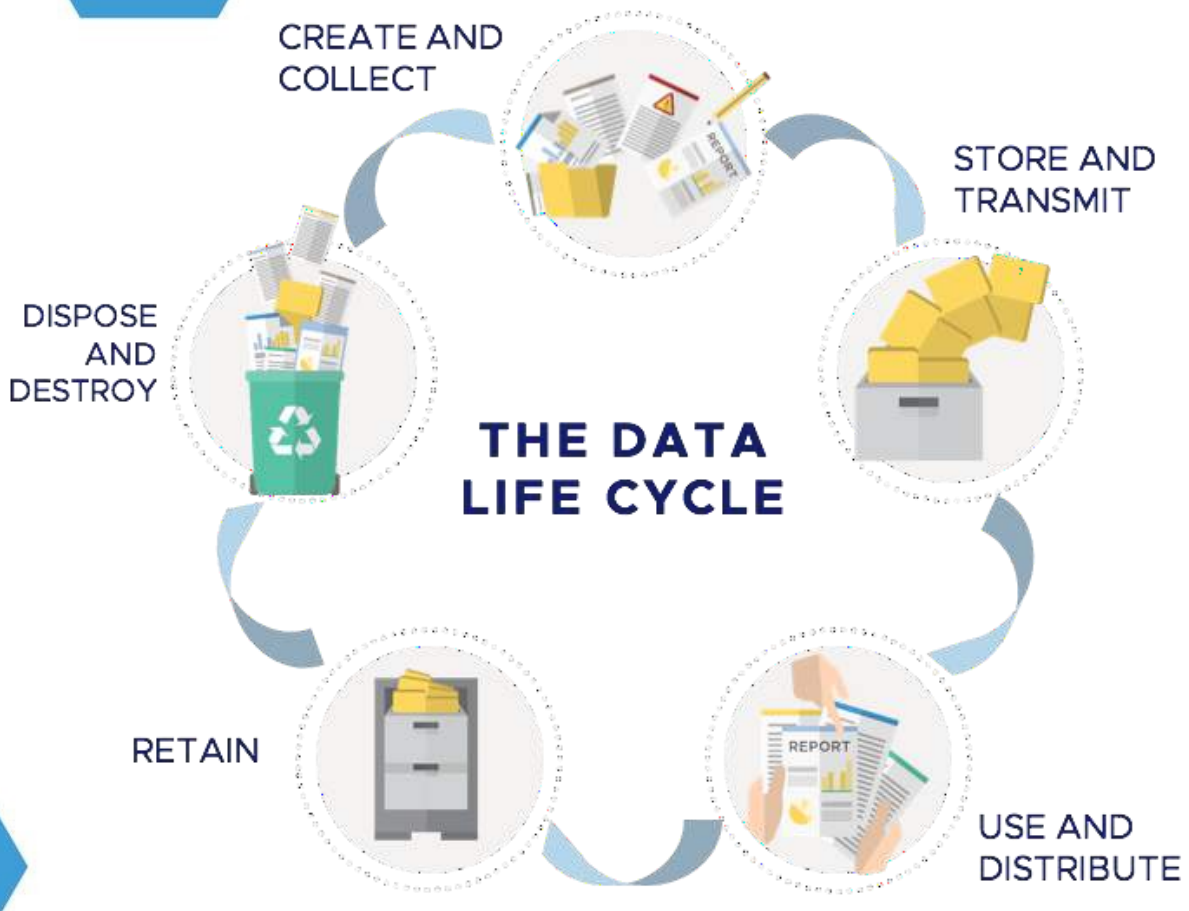
DP 15

NON-BANK FINANCIAL INSTITUTIONS

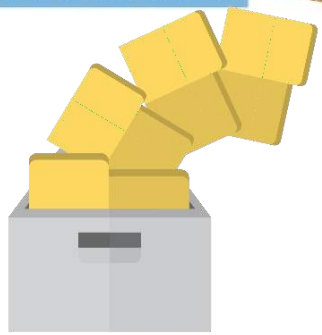


I. CREATE AND COLLECT

DP 15
NON-BANK FINANCIAL INSTITUTIONS

Punishable Act	Imprisonment	Fine (PHP)
Unauthorized Purposes	18 months to 5 years — 2 years to 7 years	500 thousand to 2 million
Unauthorized Processing of Personal Information/Records	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million

II. STORE AND TRANSMIT



Punishable Act	Imprisonment	Fine (PHP)
Accessing of Personal Information and Sensitive Personal Information due to Negligence	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Intentional Breach	1 year to 3 years	500 thousand to 2 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 2 million

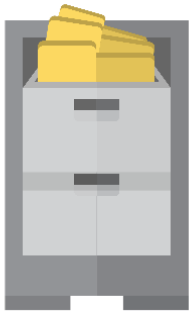
III. USE AND DISTRIBUTE

DP 15
NON-BANK FINANCIAL INSTITUTIONS

Punishable Act	Imprisonment	Fine (PHP)
Unauthorized Processing of Personal Information and Sensitive Personal Information	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Unauthorized Purposes	18 months to 5 years — 2 years to 7 years	500 thousand to 2 million
Intentional Breach	1 year to 3 years	500 thousand to 2 million
Concealing Breach	18 months to 5 years	500 thousand to 1 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 2 million

IV. RETAIN

DP 15
NON-BANK FINANCIAL INSTITUTIONS



Punishable Act	Imprisonment	Fine (PHP)
Access due to Negligence of Records	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 1 million

V. DISPOSE AND DESTROY

Punishable Act	Imprisonment	Fine (PHP)
Improper Disposal of Records	6 months 2 years — 1 year to 3 years	100 thousand to 1 million
Access due to Negligence	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Concealing Breach	18 months to 5 years	500 thousand to 1 million

Rule XI. Registration and Compliance Requirements

RA 10173 THE DATA PRIVACY ACT OF 2012

Section 46. **Enforcement of the Data Privacy Act.** Pursuant to the mandate... to administer and implement the Act, and to ensure the compliance... the Commission requires the following:

a. Registration of personal data processing systems... of at least one thousand (1,000) individuals...

b. Notification of automated processing operations... that would significantly affect the data subject;

c. Annual Report of the summary of security incidents...

d. Compliance with other requirements that may be provided in other issuances of the Commission

NATIONAL PRIVACY COMMISSION

NATIONAL
PRIVACY
COMMISSION

The NPC's 5 Pillars of Accountability and Compliance

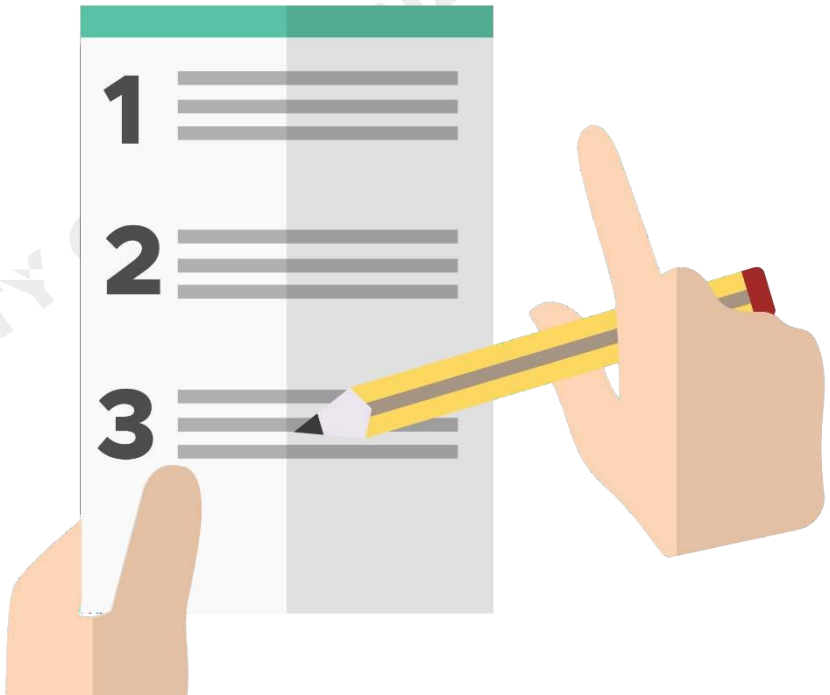
1. 
   Commit to Comply: **APPOINT A DATA PROTECTION OFFICER**
2. 
   Know Your Risks: **CONDUCT A PRIVACY RISK OR IMPACT ASSESSMENT**
3. 
   Write Your Plan: **CREATE A PRIVACY MANAGEMENT PROGRAM**
4. 
   Be Accountable: **IMPLEMENT YOUR PRIVACY AND DATA PROTECTION MEASURES**
5. 
   Be Prepared for Breach: **REGULARLY EXERCISE YOUR BREACH REPORTING PROCEDURE**

NATIONAL PRIVACY COMMISSION

DP 15
NON-BANK FINANCIAL INSTITUTIONS

INSTRUCTIONS:

Take a blank sheet of paper and number it from **1 to 20.** For each item, write **T if true, F for false,** and **D if you do not know.**



We process personal information of Filipino citizens.

We process personal information of citizens from other countries.

The total number of data subjects whose records we store is more than 250.

The total no. of data subjects whose records we store is more than 100,000.

The total number of employees in our organization is more than 1,000.

We process personal information that is classified as "sensitive" by RA 10173.

We issue unique identification numbers or documents such as passport, license, membership card.

We process personal information on paper and other analog media such as microfilm or microfiche.

We process personal information on digital media such as hard disks or servers.

The personal information that we process is scattered over several sites.

We store personal information in the cloud.

We have contracts with service providers to store or process personal information.

As of today, our organization has no privacy or data protection policies.

The personal information we keep is accessed by other companies/agencies.

The personal information we keep is accessed from other parts of the world.

The personal information we keep must be accessible 24 hours a day, 7 days a week.

There is a sub-second response time requirement for access to the personal information we keep.

The number of people who have access to the personal information we keep is more than 50.

The number of people who have access to the personal information we keep is more than 250.

We have ongoing projects where we use personal information in big data or data analytics.

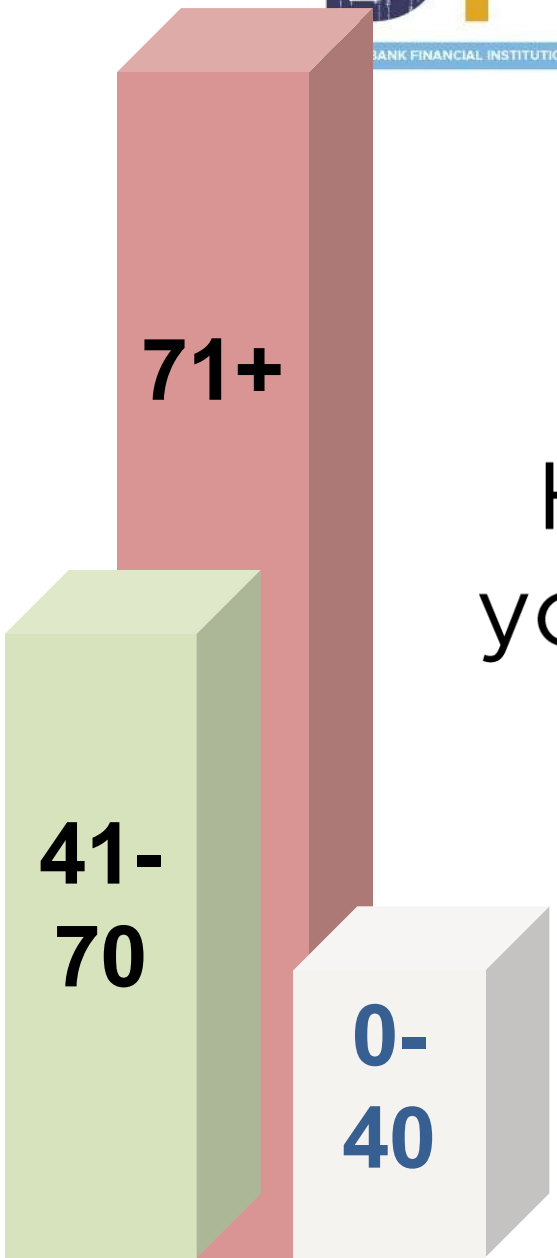
LET US SCORE!

You get **five (5)** points for every **T**

You get **five (5)** points for every **D**

DP 15

BANK FINANCIAL INSTITUTIONS



How did you score?

NATIONAL PRIVACY COMMISSION

DP 15
NON-BANK FINANCIAL INSTITUTIONS

PRIVACY RISK	BENEFIT	CONTROLS	IMPACT ASSESSMENT
High	Low		Unacceptable
Medium	Medium	High	Unreasonable
Low	High	Low	Acceptable
Medium	Medium	Medium	Acceptable

Privacy risk is the probability that the data processing or other activity involving data will result in a loss of the rights and freedoms of an individual.

THE NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK

I. GOVERNANCE

A. Choose a DPO

II. RISK ASSESSMENT

B. Register
C. Records of processing activities
D. Conduct PIA

III. ORGANIZATION

E. Privacy Management Program
F. Privacy Manual

IV. DAY TO DAY

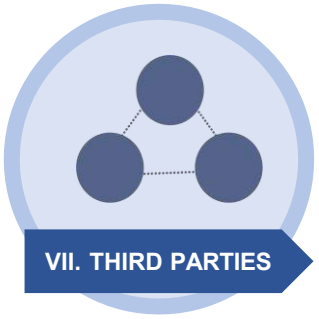
G. Privacy Notice
H-O. Data Subject Rights
P. Data Life Cycle

V. DATA SECURITY

Q. Organizational
R. Physical
S. Technical
- Data Center
- Encryption
- Access Control Policy

VI. BREACHES

T. Data Breach Management;
- Security Policy
- Data Breach Response Team
- Incident Response Procedure
- Document
- Breach Notification



VII. THIRD PARTIES

U. Third Parties;
- Legal Basis for Disclosure
- Data Sharing Agreements
- Cross Border Transfer Agreement

VIII. MANAGE HR

V. Trainings and Certifications
W. Security Clearance

IX. CONTINUITY

X. Continuing Assessment and Development
- Regular PIA
- Review Contracts
- Internal Assessments
- Review PMP
- Accreditations

X. PRIVACY ECOSYSTEM

Y. New technologies and standards
Z. New legal requirements

THE NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE CHECKLIST

I. Establishing Data Privacy Governance

1. Appointment of your Data Privacy Officer (DPO)

II. Risk Assessment

2. Register
3. Records of processing activities
4. Conduct of a Privacy Impact Assessment (PIA)

III. Preparing Your Organization's Data Privacy Rules

5. Formulate your organization's privacy management program (PMP)
6. Craft your agency's privacy manual

IV. Privacy in Day-to-Day Information Life Cycle Operations (To Be Included in the Privacy Manual)

7. Informing data subjects of your personal information processing activities and obtain their consent, when necessary. (Privacy Notice)
8. Formulation of policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them
9. Policies for limiting data processing according to its declared, specified and legitimate purpose
10. Policies/procedures for providing data subjects with access to their personal information including its sources, recipients, method of collection, purpose of disclosure to third parties, automated processes, date of last access, and identity of the controller (Data Subject Access Request)
11. Policies/procedures that allow data subjects to dispute inaccuracy or error of their personal information including policies/procedures to keep the same up to date
12. Policies/procedures that allow a data subject to suspend withdraw or order the blocking, removal or destruction of their personal information

CREATION AND COLLECTION, STORAGE, TRANSMISSION, USE AND DISTRIBUTION, RETENTION, AND DESTRUCTION/ DISPOSAL

THE NPC'S 32-Pt. DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE CHECKLIST

20. Compliance with the DPA's Data Breach Management Requirements (e.g. Security Policy, Data Breach Response Team, Incident Response Procedure, Document, Breach Notification)

VII. Managing Third Party Risks

21. Maintaining data privacy requirements (Legal Basis for Disclosure, Data Sharing Agreements, Cross Border, Security of Transfers) for third parties (e.g. clients, vendors, processors, affiliates)

VIII. Managing Human Resources (HR)

22. Periodic and mandatory personnel training on privacy and data protection in general and in areas reflecting job-specific content
23. Issuance of Security Clearance for those handling personal data

IX. Continuing Assessment and Development

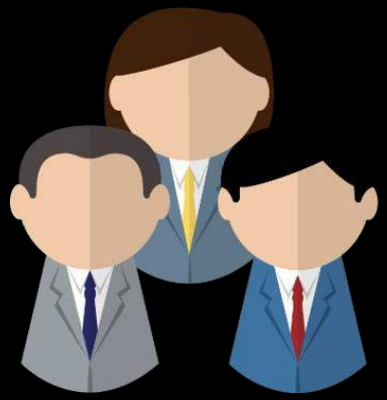
24. Scheduling of Regular PIA for new and existing programs, systems, processes and projects
25. Review of Forms, Contracts, Policies and Procedures on a regular basis
26. Scheduling of Regular Compliance Monitoring, Internal Assessments and Security Audits
27. Review, validation and update of Privacy Manual
28. Regular evaluation of Privacy Management Program
29. Establishing a culture of privacy by obtaining certifications or accreditations vis-à-vis existing international standards

X. Managing Privacy Ecosystem

30. Monitoring of emerging technologies, new risks of data processing, and the Privacy Ecosystem
31. Keeping track of data privacy best practices, sector specific standards, and international data protection standards
32. Seeking guidance and legal opinion on new National Privacy Commission (NPC) issuances or requirements

AREA I. Establishing Data Privacy Governance

Item #1. Appoint Data Protection Officer



AREA II. Risk Assessment

Item #2. Register

Item #3. Records of Processing Activities

Item #4. Conduct of a Privacy Impact Assessment (PIA)

AREA III. Preparing Your Organization's Data Privacy Rules

Item #5. Formulate your organization's privacy management program (PMP)

Item #6. Develop your agency's privacy manual and complaints mechanism

NATIONAL PRIVACY COMMISSION

AREA IV: Privacy in Day-to-Day Information Life Cycle Operation

Item #7. Informing data subjects of your personal processing activities and obtain their consent, when necessary.

Item #8. Formulation of policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them.

Item #9. Policies for limiting data processing according to its declared, specified and legitimate purpose.

Item #10. Policies/ procedure providing data subjects with access to their personal information including its sources, recipient, method of collection, purpose of disclosure to third parties, automated processes, date of last access, and identity of controller

Item #11. Policies/procedure that allow data subjects to dispute accuracy or error of their personal information including policies/procedure to keep the same up to date.

Item #12. Policies/ procedure that allow data subjects to suspend, withdraw or order the blocking, removal or destruction of their personal information.

Item #13. Policies/procedure for accepting and addressing complaints from data subjects.

Item #14. Policies/procedures that allow data subjects to get indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false and unlawfully obtained or unauthorized use of personal information.

Item #15. Policies/procedures that allow data subjects to obtain from the personal information controller a copy of his or her personal data processed by electronic means and in a structured and commonly used format.

Item #16. Policies/procedures for creation and collection, storage, transmission, use and distribution, retaining personal data for only a limited period or until the purpose of the processing has been achieved, and ensuring that data is securely destroyed or disposed of

NATIONAL PRIVACY COMMISSION

AREA V. Managing Personal Data Security Risk

Item #17. Implement appropriate and sufficient organizational security measures
Item #18. Implement appropriate and sufficient physical security measures
Item #19. Implement appropriate and sufficient technical security measures

AREA VI. Data Breach Management

Item #20. Compliance with the DPA's Data Breach Management Requirements

AREA VII: Managing Third Party Risk

Item #21: Maintaining data privacy requirements for third parties (e.g. clients, vendor, processor, affiliates)? (Compliance, Agreement, Due Diligence, Notifications, Access Policies.)

AREA VIII. Managing Human Resources (HR)

Item #22. Periodic and mandatory personnel training on privacy and data protection in general and in areas reflecting job-specific content
Item #23. Issuance of Security Clearance for those handling personal data

AREA IX. Continuing Assessment and Development

Item #24. Scheduling of Regular PIA for new and existing programs, systems, processes and projects
Item #25. Review of Forms, Contracts, Policies and Procedures on a regular basis
Item #26. Scheduling of Regular Compliance Monitoring, Internal Assessments and Security Audits
Item #27. Review, validation and update of Privacy Manual
Item #28. Regular evaluation of Privacy Management Program
Item #29. Establishing a culture of privacy by obtaining certifications or accreditations vis-à-vis existing international standards

AREA X. Managing Privacy Ecosystem

Item #30. Monitoring of emerging technologies, new risks of data processing, and the Privacy Ecosystem
Item #31. Keeping track of data privacy best practices, sector specific standards, and international data protection standards
Item #32. Seeking guidance and legal opinion on new National Privacy Commission (NPC) issuances or requirements

DP 15

NON-BANK FINANCIAL INSTITUTIONS

What do we look for when the NPC comes knocking at your door?

1. Can we feel a culture of **Privacy**?
2. Do you have a **sensible data privacy program**?
3. Is it based on **risk assessment**?
4. Do you **train your staff in data privacy** and protection?
5. Are you prepared for **breach**?

Cultivating a Culture of Trust

DP 15

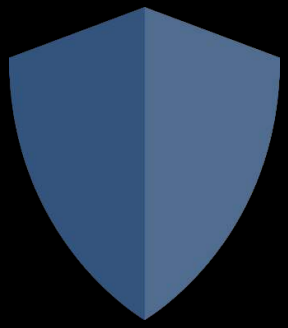
NON-BANK FINANCIAL INSTITUTIONS

NATIONAL PRIVACY COMMISSION

Building a regime of Trust

NATIONAL PRIVACY COMMISSION

The Data Privacy Golden Rule



If you Can't Protect It...

DONT Collect It.

NATIONAL PRIVACY COMMISSION