Role of DPO and Compliance Framework

Dr. Rolando R. Lansigan,
Chief, Compliance and Monitoring Division

NATIONAL PRIVACY COMMISSION

DP 14

5 PILLARS OF COMPLIANCE

1	2	3	4	5
Appoint a Data Protection Officer	Conduct a Privacy Impact Assessment	Create a Privacy Management Program	Implement Data Privacy and Security Measures	Be ready in case of a Data Breach

NATIONAL PRIVACY COMMISSION

DP 14

#1: Appoint a DPO (Data Protection Officer)

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

What compliance looks like	What negligence looks like
Notarized appointment or designation of a DPO, filed with the NPC	Lack of interaction between DPO and top management, between DPO and functional units
Evidence of actions taken on basis of DPO recommendations	Inaction on complaints from data subjects
Contact details on website (if any)	Non-reporting to NPC
Continuing education program	

DPO Selection Considerations

Minimum requirements

- knowledge of privacy principles and data protection practices
- empowered to be a change agent

Options

- supported by a team or a committee
- full-blown task force or data protection office

NATIONAL PRIVACY COMMISSION

DP 14

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. advice 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);

What does a COP do?

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.

NATIONAL PRIVACY COMMISSION

DP 14

Who is allowed to designate a COP?
(See NPC Advisory 17-01)

- Local Government Units (LGUs). Each LGU shall designate a DPO. However, a component city, municipality, or barangay is allowed to designate a COP, provided that the latter shall be under the supervision of the DPO of the corresponding province, city, or municipality that that component city, municipality or barangay forms part of.
- Government Agencies. Each government agency shall designate a DPO. Where a government agency has regional, provincial, district, city, municipal offices, or any other similar sub-units, it may designate or appoint COPs for each sub-unit. The COPs shall be under the supervision of the DPO.
- Private Sector. Where a private entity has branches, sub-offices, or any other component units, it may also appoint or designate a COP for each component unit.

  Subject to the approval of the NPC, a group of related companies may appoint or designate the DPO of one of its members to be primarily accountable for ensuring the compliance of the entire group with all data protection policies. Where such common DPO is allowed by the NPC, the other members of the group must still have a COP, as defined in this Advisory.
- Other Analogous Cases. PICs or PIPs that are under similar or analogous circumstances may also seek the approval of the NPC for the appointment or designation of a COP, in lieu of a DPO.

What DPO might need to build capacity

- ✓A support group
- ✓A mentor
- ✓An IT security audit
- ✓Litigation support
- ✓Access to top management
- ✓Continuing education
- ✓Organizational leverage
- ✓Tool support
- ✓Support staff

NATIONAL PRIVACY COMMISSION

DP 14

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

NATIONAL PRIVACY COMMISSION

DP 14

THE NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE CHECKLIST

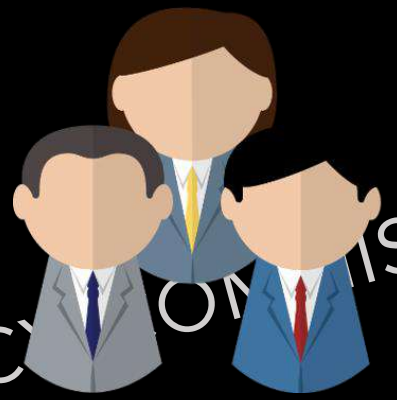
I. Establishing Data Privacy Governance	
1. Appointment of your Data Privacy Officer (DPO)	
II. Risk Assessment	
2. Register	
3. Records of processing activities	
4. Conduct of a Privacy Impact Assessment (PIA)	
III. Preparing Your Organization's Data Privacy Rules	
5. Formulate your organization's privacy 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	CREATION AND COLLECTION, STORAGE, TRANSMISSION, USE AND DISTRIBUTION, RETENTION, AND DESTRUCTION/ DISPOSAL
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	

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)

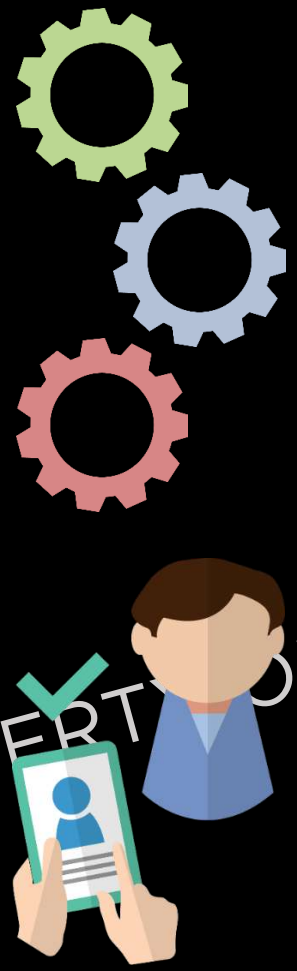
AREA III. Preparing Your Organization's Data Privacy Rules

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

NATIONAL PRIVACY COMMISSION

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

Thank you! Any questions?

info@privacy.gov.ph