THE 90 DAY PLAN

Raymund Enriquez Liboro
Privacy Commissioner
National Privacy Commission
THE DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK

1. Choose a DPO
2. Register

GOVERNANCE

3. Conduct PIA

RISK ASSESSMENT

4. Privacy Management Program
5. Privacy Manual

ORGANIZATION

6. Privacy Notice
7-12. Data Subject Rights
13. Retention
14. Disposal

DAY TO DAY

15. Data Center
16. Encryption
17. Access Policy
18. Transfers

DATA SECURITY

19. Breach Management:
   - Assessment Monitoring
   - Response Team
   - Review
   - Notification

BREACHES

20. Third Parties:
   - Due Diligence
   - Agreements
   - Notification
   - Access Policy

THIRD PARTIES

21. Training

MANAGE HR

22. Conduct and update PIA

PROJECTS

23. Monitor Legal Compliance
   • Contract Review

MANAGE LEGAL
30 DAYS:
- Conduct a *Privacy Impact Assessment* & formulate a *Personal Data Inventory*
III. PREPARING YOUR ORGANIZATION’S DATA PRIVACY RULES

30 DAYS:

- Formulate your organization's Privacy Policy
- Formulate your organization's Control Framework for Data Protection & Remediation Roadmap
IV. PRIVACY IN DAY-TO-DAY INFORMATION LIFE CYCLE OPERATIONS

CREATION / COLLECTION STAGE

30 DAYS:

- Inform data subjects of your personal information processing activities & obtain their consent, when necessary
- (Privacy Notice)
- Formulate policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them
STORAGE / TRANSMISSION & USE / DISTRIBUTION STAGES

30 DAYS:
Develop policies/procedures:

- for limiting data processing according to its declared, specified and legitimate purpose
- 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, & identity of the controller
that allow data subjects to **dispute inaccuracy or error** of their personal information including policies/procedures to keep the same up to date

- that allow data subjects to **suspend, withdraw or order the blocking, removal or destruction** of their personal information if outdated, false, unlawfully obtained, unnecessary or used for unauthorized purposes

- for **accepting and addressing complaints** from data subjects
RETENTION STAGES

30 DAYS:

- Develop policies/procedures for retaining personal data for only a **limited period** or until the purpose of the processing has been achieved
DESTRUCTION / DISPOSAL STAGES

30 DAYS:

- Develop policies/procedures for ensuring that data is securely destroyed or disposed of.
V. MANAGING INFORMATION SECURITY RISK

60 DAYS:
- Comply with the DPA's data storage requirements
- Comply with the DPA's control access requirements for personal data (onsite, remotely or online)
- Comply with the DPA's requirements for personal data transfers
VI. DATA BREACH MANAGEMENT PROGRAM

60 DAYS:
- Comply with the DPA's Data Breach Management requirements
VII. MANAGING THIRD PARTY RISK

90 DAYS:
- Maintain data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)
VIII. MANAGING EMPLOYEES WHO HANDLE DATA

90 DAYS:
- Conduct periodic & mandatory personnel training on privacy & data protection in general & in areas reflecting job-specific content
IX. MONITORING MECHANISMS FOR NEW & CURRENT OPERATIONAL PRACTICES

90 DAYS:
- Establish processes for the maintenance & conduct of Privacy Impact Assessment guidelines for new & existing programs, systems, processes & projects
X. MANAGING YOUR LEGAL ENVIRONMENT

90 DAYS:

- Develop policies/procedures for monitoring & complying with the applicable legal requirements in all the jurisdictions in which the organization handles data
PRIVACY.GOV.PH

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

NATIONAL PRIVACY COMMISSION