COMPLIANCE FRAMEWORK

Krishna Aira A. Tana
Compliance and Monitoring Division
Obligations of a Personal Information Controller or Processor

- UPHOLD THE RIGHTS OF DATA SUBJECTS
- ADHERE TO DATA PRIVACY PRINCIPLES
- IMPLEMENT SECURITY MEASURES
5 PILLARS OF COMPLIANCE

1. Commit to Comply: Appoint a **Data Protection Officer (DPO)**.
2. Know Your Risks: Conduct a **Privacy Impact Assessment (PIA)**.
3. Be Accountable: Create your **Privacy Management Program** and **Privacy Manual**.
4. Demonstrate Your Compliance: Implement your **privacy and data protection (PDP)** measures.
5. Be Prepared for Breach: Regularly exercise your **Breach Reporting Procedures (BRP)**.
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 Risk
R. Physical Security
S. Technical Security
- 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
I. GOVERNANCE

A. Choose a Data Protection Officer (DPO)

II. RISK ASSESSMENT

B. Register
C. Records of processing activities
D. Conduct PIA (Privacy Impact Assessment)
II. RISK ASSESSMENT

B. Register

(NPC Circular 17-01)

What to register?

Registration of your Data Processing Systems

Who should register?

A. the PIC or PIP employs at least two hundred fifty (250) employees;
B. the processing includes sensitive personal information of at least one thousand (1,000) individuals; and
C. the processing is likely to pose a risk to the rights and freedoms of data subjects.
II. RISK ASSESSMENT

B. Records of processing activities
II. RISK ASSESSMENT

B. Conduct PIA (Privacy Impact Assessment)

- What do I process and how?
- When will I re-assess?
- Do I comply with law?
- What can I do about it?
- What are the risks?
III. ORGANIZATION

E. Privacy Management Program
F. Privacy Manual
IV. DAY TO DAY

RIGHTS OF DATA SUBJECTS

- Right to be Informed
- Right to Access
- Right to Object
- Right to Rectification
- Right to Erasure or Blocking
- Right to Damages
- Right to Data Portability
- Right to File A Complaint

https://www.nks.kent.sch.uk/uploads/asset_image/2_1666.jpg
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

Q. Organizational

Involves implementing policies and programs explicitly intended to ingrain the culture of privacy into an organization’s psyche, thus making it impervious to hackers who resort to social engineering ploys.
V. DATA SECURITY

R. Physical

Refers to the practical protective schemes such as provision for security guards, padlocks, lockers and secluded archives to physically protect paper records and databases against data thieves who may resort to brute force.
Covers all proactive and defensive IT solutions an organization could employ in securing its data assets against all types of breaches. This may include the use of robust firewall and encryption systems, rigorous data access protocols, as well as anti-virus and anti-spyware solutions.
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
VII. THIRD PARTIES

Outsourcing Agreement

- shall set out the subject-matter and duration of the processing,
- the nature and purpose of the processing,
- the type of personal data and categories of data subjects,
- the obligations and rights of the personal information controller, and
- the geographic location of the processing under the subcontracting agreement.

Legal Basis for Disclosure
VII. THIRD PARTIES

Data Sharing Agreements

Requisites:

• consent of data subjects,

• establishment of adequate safeguards for data privacy and security, and upholding of the rights of data subjects,

• provide data subjects with the required information prior to collection or before data is shared, and

• adherence to the data privacy principles.
A personal information controller shall be responsible for any personal data under its control or custody, including information that have been outsourced or transferred to a personal information processor or a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.
V. Trainings and Certifications
W. Security Clearance
IX. CONTINUITY

X. Continuing Assessment and Development

- Regular PIA (Private Impact Assessment)
- Review Contracts
- Internal Assessments
- Review and update PMP and Privacy Manual
X. PRIVACY ECOSYSTEM

Y. New technologies and standards
Z. New legal requirements
If you can't protect it, don't collect it.
The Data Privacy Golden Rule
Thank you!

NATIONAL PRIVACY COMMISSION