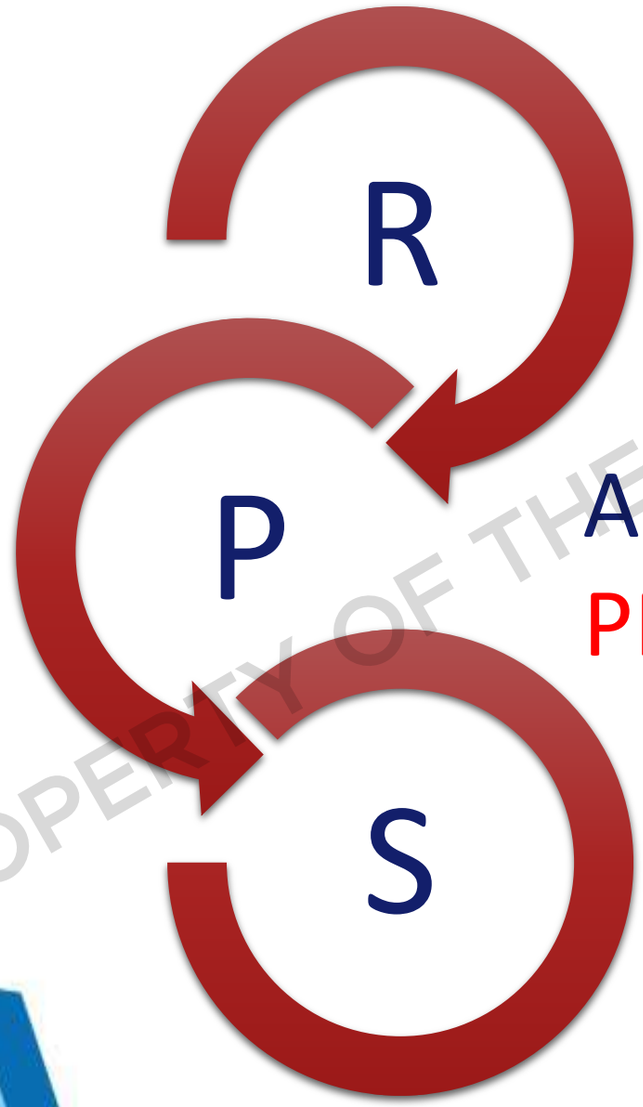
COMPLIANCE FRAMEWORK

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

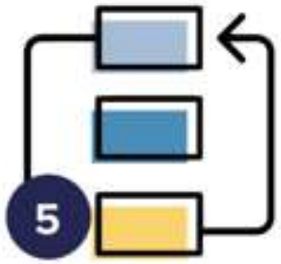
DPO 2O

Commit to Comply: Appoint a **Data Protection Officer** (DPO).

Know Your Risks: Conduct a **Privacy Impact Assessment** (PIA).

Be Accountable: Create your **Privacy Management Program** and **Privacy Manual**.

Demonstrate Your Compliance: Implement your **privacy and data protection** (PDP) measures.



Be Prepared for Breach: Regularly exercise your **Breach Reporting Procedures** (BRP).

5 PILLARS OF COMPLIANCE

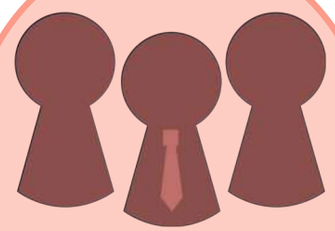
THE NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK

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

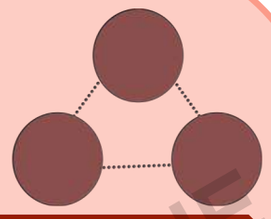
G. Privacy Notice
H-O. Data Subject Rights
P. Data Life Cycle

V. DATA SECURITY

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

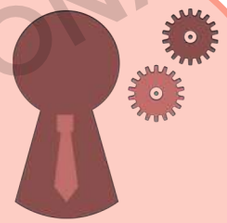
VI. BREACHES

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

DPO

NATIONAL PRIVACY COMMISSION

I. GOVERNANCE

https://litmosheroes.com/wp-content/uploads/2018/03/GDPR-Quiz-Question-6.jpg

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?

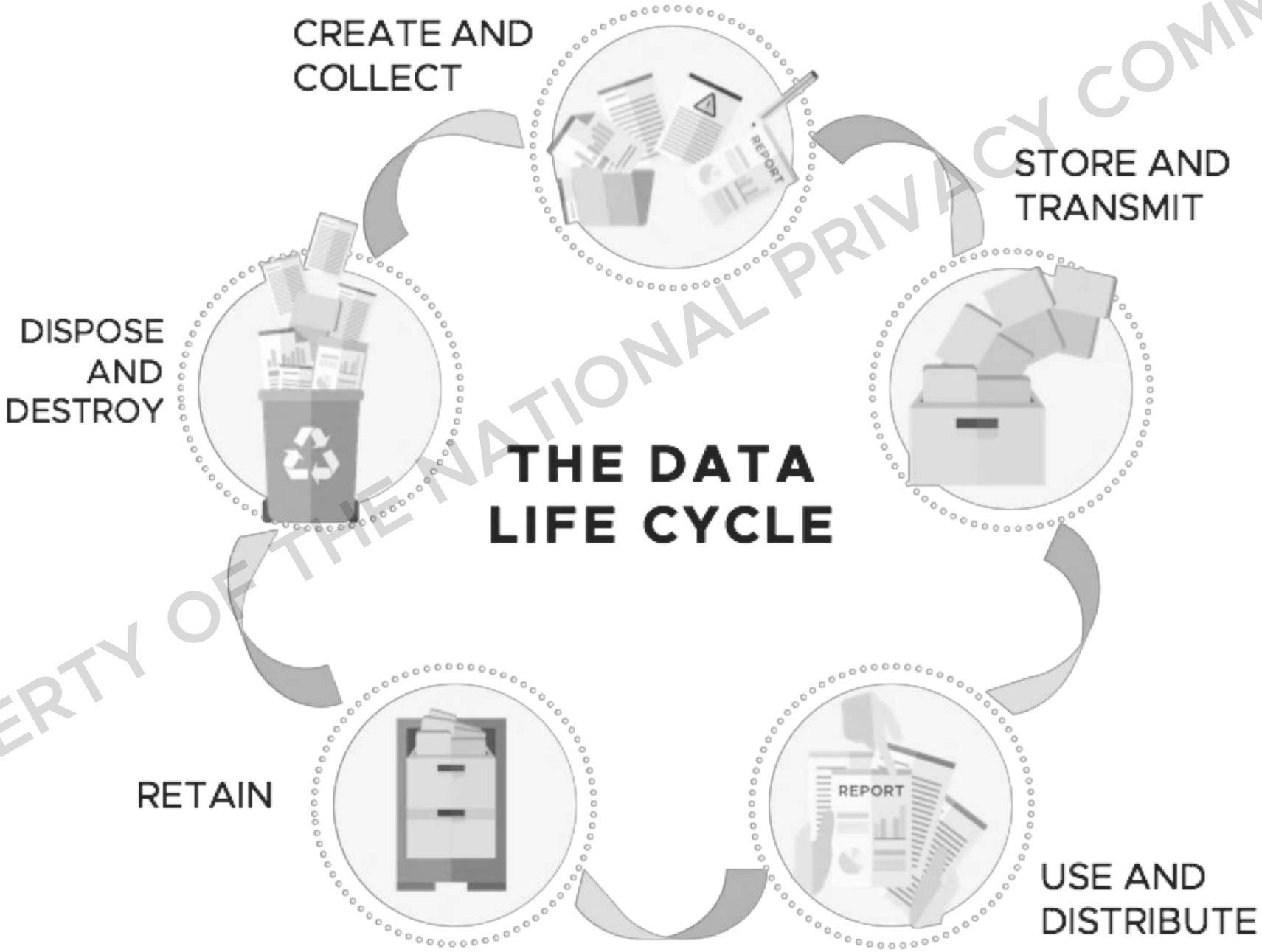
Registration of your Data Processing Systems

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)

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

http://www.gordiandynamics.com/wp-content/uploads/2015/08/data-security-animation.jpg

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

V. DATA SECURITY

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.

V. DATA SECURITY

S. Technical

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

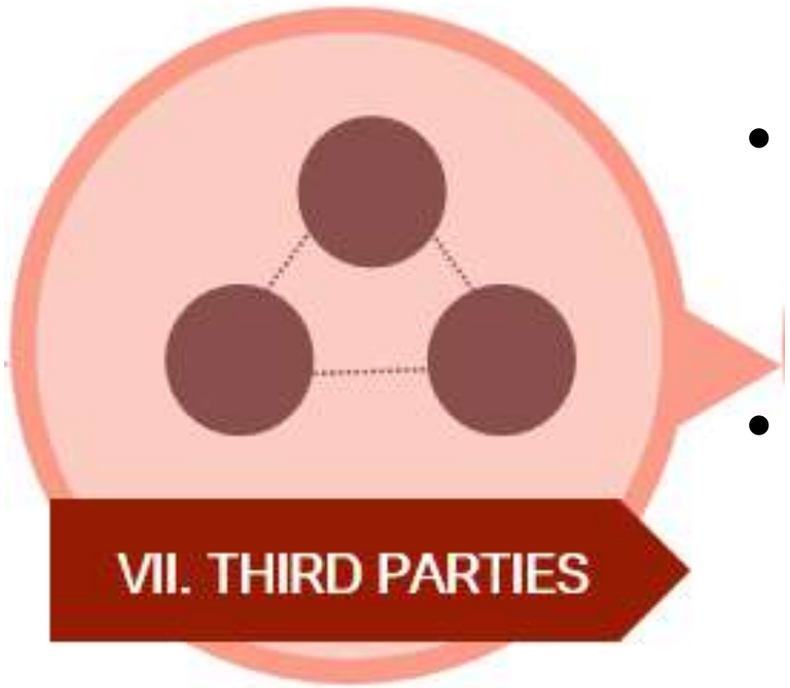
VII. THIRD PARTIES

U. Third Parties;

- Legal Basis for Disclosure
- Data Sharing Agreements
- Cross Border Transfer Agreement

http://infoorel.ru/user_foto/news/01906e8be48ab7b9c6903f1e751df0d7.jpeg

VII. THIRD PARTIES

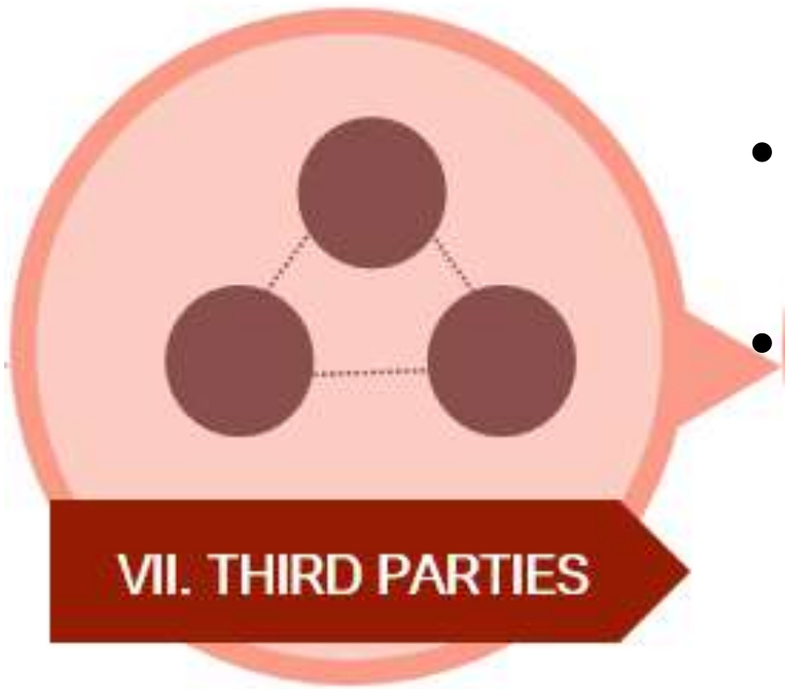


Legal Basis for Disclosure

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.**

VII. THIRD PARTIES

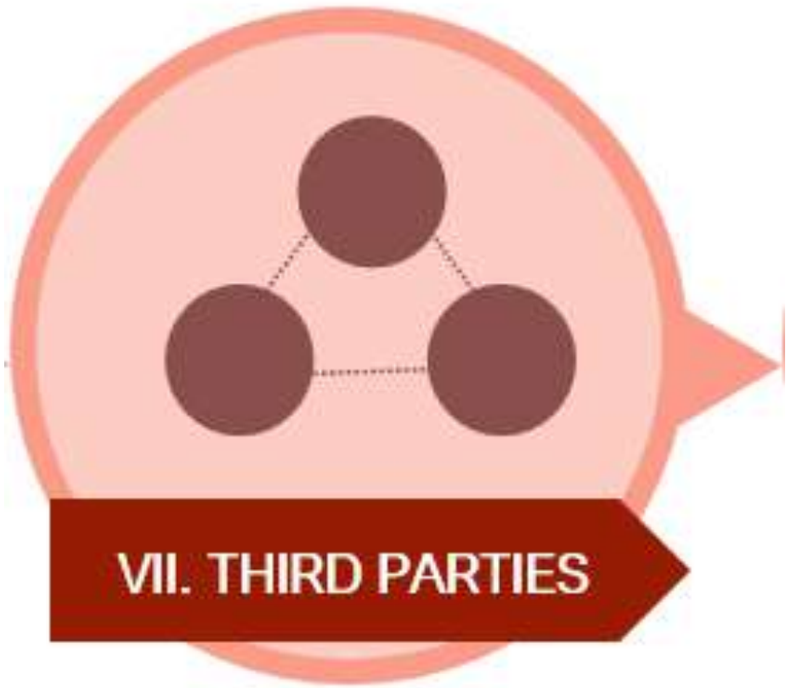


Requisites:

- **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.**

Data Sharing Agreements

VII. THIRD PARTIES



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.

Cross Border Transfer Agreement

VIII. MANAGE HR

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

DP 20
REAL ESTATE

If you can't protect it, don't collect it.

The Data Privacy Golden Rule

NATIONAL
PRIVACY
COMMISSION

Thank you!