"NPC Circular 16-01 :

SECURITY OF PERSONAL DATA IN GOVERNMENT AGENCIES"

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 2018

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

Government Requirements based on NPC Circular 16-01

Section 4 :

- **Appointment Papers of a Data Protection Officer :**
  - A designated individual(s) who is accountable for the organization's compliance with the DPA

- **Privacy and data protection policies :**
  - Create privacy and data protection policies

Section 5 :

Privacy Impact Assessments:

-Conduct a privacy impact assessment for each program or process to determine the privacy risks and legal gaps

Section 6 :

. **Control Framework for RISKS and LEGAL GAPS :**

Address the risks and legal gaps identified in the privacy impact assessments by creating a control framework with proper organizational, physical and technical security measures

Cont. of Section 6 :

- **ISO/IEC 27002 (recommended):**

For large-scale agencies (more than 1,000 employees), it is recommended to implement the use of ISO/IEC 27002 – Code of practice for information security controls

Section 7 :

Data Center:

Personal data being processed by a government agency shall be stored in a data center with the appropriate control framework for data protection

Section 8:

Encryption of personal data at rest and in transit (AES-256):

Personal data that are processed digitally, at rest and in transit, must be encrypted using Advanced Encryption Standard with a key size of 256 bits as minimum standard

---

Password policy:

Enforcement of a strong and sufficient password policy to deter passwords attacks

Section 9:

Access Control Policy:

Access to all applications, processing systems and facilities owned and controlled by an agency shall be restricted to its personnel that have the appropriate security clearance.

Section 10:

Outsourcing Contracts:

When dealing with personal information processors, ensure that proper organizational, physical and technical security measures are in place to ensure the confidentiality, integrity and availability of personal data

Section 11:

Audits:

To further ensure personal data protection, NPC reserves the right to conduct an audit. An independent verification/certification by a reputable third party may also be accepted.

Section 12:

ISO/IEC 27018 certification (recommended):

An ISO/IEC 27018 certification is recommended for the service or function provided by a service provider.

Section 13:

Archives:

Apply organizational, physical and technical security measures to protect archived personal data

Section 14-15:

Access Control and Security Clearance for Database Modification or Personal Data Access :

Strictly regulate access to personal data by having a security clearance policy for personal data that are in the agency's custody

Section 16:

Access Control Policy on Outsourced Providers

Contractors, consultants and service providers that have access to personal data shall be governed by strict procedures stated in their contracts

Section 17-18:

Acceptable Use Policy

Have an up-to-date acceptable use policy regarding the use of ICT resources

Cont. of Section 17-18:

Secure Encrypted link and Multi-Factor Authentication for Online Access

Agency personnel who access personal data online should authenticate their identity through a secure encrypted link and use multi-factor authentication.

Section 19:

Automatic Deletion

Provide for the automatic deletion of temporary files that may be stored on a local machine

Cont. of Section 19:

Network Drive

Personnel shall only be permitted to save personal data to an allocated network drive whenever applicable

---

Drives and USB ports (disabling policy)

Establish policies to prevent unlawful personal data distribution through portable media

Section 20:

Authorized Devices Policy

Ensure that only authorized devices are being used.

Section 21:

Remote Wipe/Deletion Policy

Adopt and use technologies that allow the remote disconnection of a mobile device owned by the agency or the deletion of personal data in it.

Section 22:

Paper-based Filing System

Maintain a log for personal data that are stored in paper files or any physical media.

Section 24:

Email Encryption

If personal data are transferred by email, data must be encrypted

Section 25:

Policies on printing personal data

Controls must be in place to prevent personnel from printing or copying personal data to personal productivity software like word processors and spreadsheets.

Section 26:

Full Disk Drive Encryption

Ensure that the agency utilizes full disk encryption whenever portable media are used for personal data processing.

Section 27:

One-time PIN for CD or DVD usage or distribution

If the use of compact discs in personal data transfer is unavoidable, an authentication technology such as one-time PIN (OTP) must be in place.

Section 28:

Fax Machines

Facsimile technology shall not be used for transmitting documents containing personal data.

Section 29:

Post Mail usage policy

Organizational, physical and technical measures should be adopted in transmitting documents or media containing personal data by mail or post.

Section 31:

Disposal Policy

Procedures must be established regarding secure disposal of personal data stored onsite (files and computer equipment) and offsite.

Section 33:

Data Breach Management

Establish data breach management procedures

For more information, please visit :

PRIVACY.GOV.PH

Like and follow us at :

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