DATA PRIVACY ACT (DPA) QUICK GUIDE

WHAT IS THE DPA?

Fully titled, "An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes" the DPA aims to protect the fundamental human right of privacy, of communication while ensuring the free flow of information to promote innovation and growth.

KEY DPA ACTORS

National Privacy Commission NPC
independent body mandated to implement the DPA

Data subject
an individual whose personal data is processed

Personal information controller PIC
a natural or juridical person, or any other body who controls the processing of personal data

Personal information processor PIP
a natural or juridical person, or any other body to whom a PIC may outsource or instruct the processing of personal data

WHAT IS PERSONAL INFORMATION (PI)?

PI refers to any information from which the identity of an individual is apparent or can be reasonably and directly ascertained, or when put together with other information would directly and certainly identify an individual

CRITERIA FOR LAWFUL PROCESSING OF PI

- Consent
- Contract with the individual
- Vital interests/Life & health
- Legal obligation
- National emergency / public order & safety, as prescribed by law
- Constitutional or statutory mandate of a public authority
- Legitimate interests of the PIC or third parties

WHAT ARE A PIC OR PIP'S PRIMARY OBLIGATIONS?

☐ **Adhere to data privacy principles**

Transparency | Legitimate purpose | Proportionality

☐ **Uphold data subject rights**

- Information
- Access
- Data Portability
- Rectification
- Erasure or blocking
- To object
- To file a complaint
- To damages

☐ **Implement security measures**

Organizational | Physical | Technical

5 PILLARS OF DATA PRIVACY ACCOUNTABILITY & COMPLIANCE

Pillar	Reference
1. Appoint a Data Protection Officer	NPC Advisory 2017-01
2. Conduct a Privacy Impact Assessment	NPC Advisory 2017-03
3. Have a Privacy Management Program & codify it into a Privacy Manual	PMP Guide in NPC Privacy Toolkit
4. Implement data privacy & protection measures	NPC Circular 2016-01; DPAC in NPC Privacy Toolkit
5. Exercise Breach Reporting Procedures	NPC Circular 2016-03

WHAT IS SENSITIVE PERSONAL INFORMATION (SPI)?

SPI refers to info about an individual's:

- Race
- Ethnic origin
- Marital status
- Age
- Color
- Religious, philosophical or political affiliations
- Health, education, genetic or sexual life
- Proceeding for any offense committed or alleged to have been committed by an individual
- Government-issued IDs
- Those established by an executive order or an act of Congress to be kept classified

CRITERIA FOR LAWFUL PROCESSING OF SPI

- Consent
- Existing laws & regulations
- Life & health
- Processing by non-stock, non-profit orgs
- Medical treatment
- Lawful rights & interests in court proceedings/legal claims

PENALTIES

Violation	Imprisonment		Fine	
	PI	SPI	PI	SPI
Unauthorized Processing	1 – 3 years	3 – 6 years	P500,000 – P2,000,000	P500,000 – P4,000,000
Accessing Due to Negligence	1 – 3 years	3 – 6 years	P500,000 – P2,000,000	P500,000 – P4,000,000
Improper Disposal	6 months – 2 years	1 – 3 years	P100,000 – P500,000	P100,000 – P1,000,000
Processing for Unauthorized Purposes	1 year and 6 months – 5 years	2 – 7 years	P500,000 – P1,000,000	P500,000 – P2,000,000
Unauthorized Disclosure	1 – 3 years	3 – 5 years	P500,000 – P1,000,000	P1,000,000 – P5,000,000
Concealment of Security Breaches		1 year and 6 months – 5 years		P500,000 – P1,000,000
Unauthorized Access or Intentional Breach	1 – 3 years		P500,000 – P2,000,000	
Malicious Disclosure	1 year and 6 months – 5 years		P500,000 - P1,000,000	
Combination or Series of Acts	3 – 6 years		P1,000,000 – P5,000,000	

EXEMPTIONS

Applies not to the PIC/PIP but only to personal data relating to:

- Matters of public concern
- Journalistic, artistic or literary purposes
- Research purposes, intended for a public benefit
- Performance of law enforcement or rgulatory functions of public authority (e.g. Secrecy of Bank Deposits Act, Foreign Currency Deposit Act, CISA)
- Compliance of BSP-regulated banks & financial institutions with the CISA, AMLA & other applicable laws
- Residents of foreign jurisdictions w/ applicable data privacy laws

Exemptions are only allowed to the minimum extent needed to achieve purpose, w/ consideration to requirements of other regulations.

This material is downloadable at:
privacy.gov.ph/quickguide

HOW COMPLIANT ARE YOU?

Here's a checklist to find out:

Evidence of Compliance
1. Establish Data Privacy Governance
Designation/Appointment Papers/ Contract of the DPO and/or DPO team
☐ Other means to demonstrate compliance
2. Privacy Risk Assessment
☐ Inventory of personal data processing systems
☐ Visible announcement showing the contact details of DPO (e.g. website, privacy notice)
☐ Phase I - Registration Form (Notarized)
☐ Privacy Impact Assessment (PIA) report
☐ Other means to demonstrate compliance
3. Maintain Organization Commitment
☐ Privacy Manual
☐ List of activities on privacy and data protection
☐ List of key personnel assigned responsibilities for privacy and data protection within the organization
☐ Other means to demonstrate compliance
4. Privacy and Data Protection in day to day operations
☐ Valid Privacy Notice in Website and/or within organization (where collection of personal data occurs)
☐ Consent forms for collection and use of personal data
☐ List of Policies and Procedures in place that relate to privacy and data protection (may be in privacy manual)
☐ Policies and Procedure in dealing with requests for information from parties other than the data subjects (media, law enforcement, representatives)
☐ Data subjects informed of rights through privacy notices, and other means
☐ Form or platform for data subjects to request copy of their personal information and request correction
☐ Procedure for addressing complaints of data subjects
☐ Certificate of registration and notification
☐ Other means to demonstrate compliance
5. Manage Security Risks
☐ Data Center and Storage area with limited physical access
☐ Report on technical security measures and information security tools in place
☐ Firewalls used
☐ Encryption used for transmission
☐ Encryption used for storage
☐ Access Policy for onsite, remote and online access
☐ Audit logs
☐ Back-up solutions
☐ Report of Internal Security Audit or other internal assessments
☐ Certifications or accreditations maintained
☐ Vulnerability Assessment
☐ Penetration Testing for applications and network
☐ Other means to demonstrate compliance
6. Data Breach Management
☐ Schedule of breach drills
☐ Number of Trainings conducted for internal personnel on breach management
☐ Personnel Order constituting the Data Breach Response Team
☐ Incident Response Policy and Procedure (may be in Privacy Manual)
☐ Record of Security incidents and personal data breaches, including notification for personal data breaches
☐ Other means to demonstrate compliance
7. Manage Third Party Risks
☐ Data Sharing Agreements
☐ List of recipients of personal data (PIPs, other PICs, service providers, government agencies)
☐ Review of Contracts with PIPs
☐ Review of Contracts for cross-border transfers
☐ Other means to demonstrate compliance
8. Human Resources Management
☐ No. of employees who attended trainings on privacy and data protection
☐ Commitment to comply with Data Privacy Act as part of Code of Conduct or through written document to be part of employee files
☐ Certificate of Training of DPO
☐ Certifications of DPOs
☐ NDAs or confidentiality agreements
☐ Security Clearance Policy
☐ Other means to demonstrate compliance
9. Continuing Assessment and Development
☐ Policy for Conduct of PIA (may be in manual)
☐ Policy on conduct of Internal Assessments and Security Audits
☐ Privacy Manual contains policy for regular review
☐ List of activities to evaluate Privacy Management program (survey of customer, personnel assessment)
☐ Other means to demonstrate compliance
10. Manage Privacy Ecosystem
☐ No. of trainings and conferences attended on privacy and data protection
☐ Policy papers, legal or position papers, or other research initiatives on emerging technologies, data privacy best practices, sector specific standards, and international data protection standards
☐ No. of management meetings which included privacy and data protection in the agenda
☐ Other means to demonstrate compliance

5th Floor, Delegation Building
Philippine International Convention Center
PICC Complex, Roxas Boulevard, Manila, 1307

privacy.gov.ph
info@privacy.gov.ph
privacy.gov.ph
PrivacyPH
privacygovph
234-22-28

NATIONAL PRIVACY COMMISSION
An attached agency of the Department of Information and Communications Technology