Proposed
Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012"

NATIONAL PRIVACY COMMISSION

Rule I. Preliminary Provisions

- Title
- Policy
- Definitions

Rule I. Preliminary Provisions

- Title- Implementing Rules and Regulations of R.A. No. 10173, "RULES"
- Policy- Protect right to privacy and support free flow of information
- Definitions-

Personal Data

- Personal Information → identity of individual
- Sensitive Personal Information → Principle of sensitivity
- Privileged Information → Privileged Communication

Personal Information Controller

- Individual, Corporation, other body → the one who controls the processing, the one who decides
- Not the employee, Not the data protection officer, Not the Chief Information Officer

Personal Information Processor

- Individual, Corporation or other body who processed the personal data for a Personal Information Controller
- Personal information processor should not make use of personal data for its own purpose

Consent

- Data subject agrees to collection and processing of his or her personal or sensitive information, or all the parties to the exchange agrees to the collection and processing of privileged information
- The agreement was freely given, specific and proceeds from being informed of
  1. Purpose, nature and extent of processing, including intention to process personal data for scientific, statistical or research purpose
  2. Period that consent is deemed effective or instructions on how consent can be withdrawn
  3. Rights as data subject
- Consent is evidenced by written, electronic or recorded means
- Consent may also be given on behalf of the data subject by a lawful representative or an agent specifically authorized by the data subject to do so

Breach

- a security incident that leads to unlawful or unauthorized processing of personal, sensitive or privileged information, or
- a security incident that otherwise compromises the availability, integrity or confidentiality of personal data

Additional Definitions

- security incident – an event or occurrence that affects or tends to affect data protection, or that may compromise the availability, integrity and confidentiality of personal data, including those incidents that would have resulted to a security breach if not for safeguards in place
- data sharing – the disclosure or transfer of personal data under custody of a natural or juridical person or other entity involved in the processing of personal data to a third party, excludes outsourcing or instructions to personal information processor
- data processing systems – the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing
- automatic processing systems – the use of information and communications system to perform operation or set of operations on personal data under a logical framework or automated instructions

Rule II. Scope of Application

- Scope
- Non-applicability
- Protection afforded to journalists and their sources
- Protection afforded to data subjects

General Rule

- The Data Privacy Act applies to processing of personal data. (*Processing of personal data is not a right.*)
- Non-applicability shall be proven by the one asserting it.

- The Data Privacy Act shall not apply to specific categories of information, but it does not automatically mean that the personal information controller or processor is excluded from applicability.

Examples of Non-applicability

- A personal information controller can not say that he needs the consent of a government official before disclosing personal data that fall within matters of public concern.

Examples of Non-applicability

- The use of personal data for publication or exhibition is subject only to the acknowledged limits on the freedom of the press and of expression. (But when the information are stored later, adequate safeguards must be in place.)

Examples of Non-applicability

- Use for research purpose should not compromise privacy and security of personal data.

Examples of Non-applicability

- Law enforcement and regulatory agencies do not need to get the consent of the individual for the gathering of personal data in relation to a legal and authorized investigation.

Examples of Non-applicability

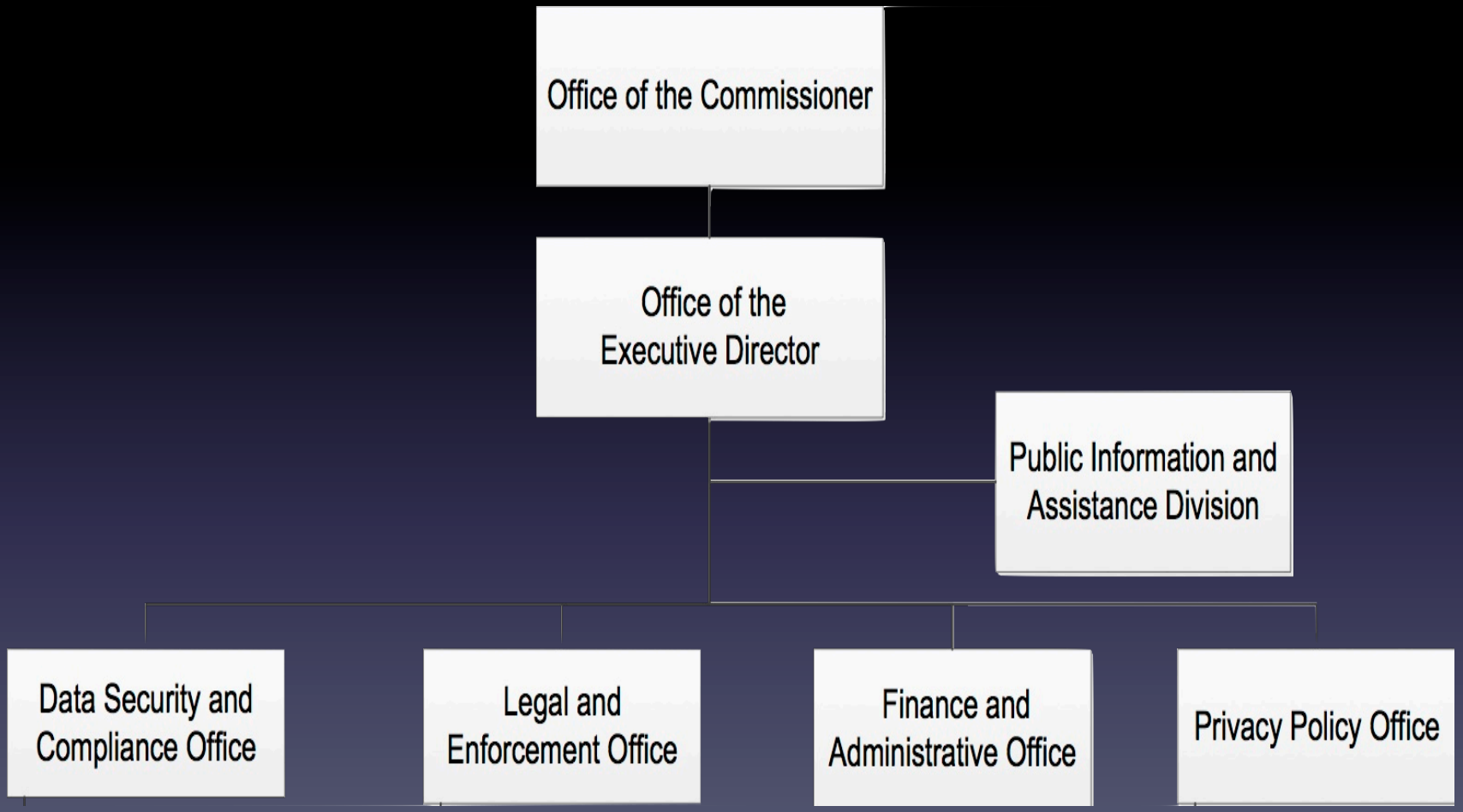
- Banks do not need consent from data subject to report covered transactions to the Anti-Money Laundering Council.
- Data sharing covered by R.A. No. 9510 (CISA) is allowed.

Examples of Non-applicability

- As long as collection of personal information of residents in a foreign country is legal or in accordance with the law, the collection shall not be inquired upon, even if information is subsequently processed in the Philippines.

Rule III. National Privacy Commission

- Mandate
- Functions
- Administrative Issuances
- Reports and Public Information
- Confidentiality of Personal Data
- Organizational Structure
- Secretariat
- Effect of Lawful Performance of Duty
- Magna Carta for Science and Technology Personnel


Office of the Commissioner
Office of the Executive Director
Public Information and Assistance Division
Data Security and Compliance Office
Legal and Enforcement Office
Finance and Administrative Office
Privacy Policy Office

Functions of the Privacy Commission

- Rule Making and Advisory
- Public Education
- Compliance and Monitoring
- Quasi-judicial (Complaints, Investigation, Enforcement)

Enforcement

- Administrative: Issue cease and desist, impose ban on processing, Compliance/ enforcement order, Impose fines and penalties
- Civil: Award indemnity
- Criminal: Recommend to DOJ only

Administrative Issuance

- Rules of procedure, suppletory application of Rules of Court
- Update minimum security standards
- Advisory or Legal opinions
- Schedule of fines and penalties

Rule IV. Data Privacy Principles

- General Principles
- Principles of Transparency, Legitimate Purpose and Proportionality
- Principles in Collection, Processing and Retention
  1. Collection must be for a specified and legitimate purpose
  2. Personal Data shall be processed fairly and lawfully
  3. Processing should ensure data quality
  4. Personal data shall not be retained longer than necessary
  5. Any authorized further processing shall have adequate safeguards
- General Principles for Data Sharing

- If you will be processing personal data, ask yourself first, are you ready to do what has to be done to protect it?
- What is your purpose?
- Are you being fair to the data subject?

Rule V. Lawful Processing of Personal Data

- Lawful Processing of Personal Information
- Lawful Processing of Sensitive Personal Information and Privileged Information
- Extension of Privileged Communication
- Surveillance of Subjects and Interception of Recording of Communications

Lawful Processing

- Personal information, in general, may be processed when data subject consents, in relation to the fulfillment of a contract, when necessary to the mandate of a public authority, or when necessary to pursue legitimate interests of controller.

Lawful Processing

- Sensitive personal information, in general, can not be processed. It may be allowed if data subject consents, when its processing is necessary to save lives, or when it is otherwise specifically authorized by law.

Rule VI. Security Measures for Data Protection

- Data Privacy and Security
- Organizational Security
- Physical Security
- Technical Security
- Appropriate Level of Security

- The obligation to put in place security measures for data protection falls on both the personal information controller and personal information processor.
- Security measures: organizational, physical and technical - to maintain confidentiality, integrity and availability of personal data, and prevent unauthorized processing

Rule VII. Data Privacy and Security in Government.

- Responsibility of Heads of Agencies
- Requirements Relating to Access by Agency Personnel to Sensitive Personal Information
- Implementation of Security Requirements
- Applicability to Government Contractors

- Responsibility of Heads of Agencies – secure sensitive personal data in government
- Approve on-line and off-site access by government employee
- Registration of data processing systems (given one year period to complete registration)

Rule VIII. Rights of Data Subject

- Rights of the Data Subject
  1. Right to be informed
  2. Right to object
  3. Right to access
  4. Right to correct
  5. Right to rectification, erasure or blocking
- Transmissibility of Rights of the Data Subject
- Right to Data Portability
- Limitation on Rights – statistical and scientific research, investigations

- A Data Subject may file a complaint with the National Privacy Commission for violation of his or her rights.
- The National Privacy Commission will facilitate or enable settlement of complaints.

Rule IX. Data Breach Notification.

- Data Breach Notification
- Contents of Notification
- Delay of Notification
- Breach Report
- Procedure for Notification

Breach Notification

- Who? Personal Information Controller
- When? Within 24 hours of knowledge or reasonable belief that breach has occurred, where real risk of serious harm to data subjects likely
- What? The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach.

Rule X. Outsourcing and Subcontracting Agreements.

- Subcontract of Personal Data
- Agreements for Outsourcing
- Duty of Personal Information Processor

- The personal information controller has the duty to review its outsourcing agreements, to ensure that proper safeguards are in place when it outsources or subcontracts processing of personal data.

Rule XI. Registration and Compliance Requirements

- Enforcement of the Data Privacy Act
- Registration of Data Processing Systems
- Notification for Automatic Processing Operations
- Approval of Data Sharing Agreements
- Review by the Commission

Rule XII. Rules on Accountability

- Accountability for Transfer of Personal Information
- Accountability for Violation of the Act, these Rules and other issuances

Rule XIII. Penalties

- Unauthorized Processing of Personal Information and Sensitive Personal Information
- Accessing Personal Information and Sensitive Personal Information Due to Negligence
- Improper Disposal of Personal Information and Sensitive Personal Information
- Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes
- Unauthorized Access or Intentional Breach
- Concealment of Security Breaches Involving Sensitive Personal Information

Rule XIII. Penalties

- Malicious Disclosure*
- Unauthorized Disclosure*
- Combination or Series of Acts
- Extent of Liability
- Large-Scale
- Offense Committed by Public Officer
- Restitution
- Fines and Penalties

Rule XIV. Miscellaneous Provisions

- Appeal
- Period for Compliance
- Interpretation
- Separability Clause
- Repealing Clause
- Effectivity Clause

What to Do Now

- Adhere to principles of transparency, legitimate purpose and proportionality
- Adopt a Privacy Policy
- Implement security measures in accordance with industry standards
- Notification in case of security breach
- Uphold rights of data subjects
- Seek advice for privacy concerns - data sharing agreements, research

COMMENTS/RECOMMENDATIONS

- IRR

http://www.gov.ph/2016/06/20/irr-data-privacy-act-2012/

- COMMENTS

info@privacy.gov.ph

- SUBMIT ONLINE

privacyph.org/submitquestion

- Discuss using

#privacyPH