LIGHTS Institute

Data Privacy Act of 2012

Memory Guide for the 2020/21 Bar Exams

Atty. Ivy Patdu, *former Deputy Privacy Commissioner, NPC*
Atty. Jam Jacob, *former Head of Privacy Policy Office, NPC*

State Policy

To protect the right to privacy while ensuring free flow of information.

Key Definitions

Consent - freely given, specific, informed indication of will, where the data subject agrees to the processing of his/her personal data.

Data subject (DS) - individual whose personal data is processed.

Personal information – information about an identified or identifiable natural person

Personal information controller (PIC) - a person or organization who controls the processing of personal data. It excludes:

- Those merely instructed to process personal data; and
- Individual who processes for his/her personal, family or household affairs.

Personal information processor (PIP) – a person or organization to whom a PIC may outsource the processing of personal data.

Processing - any operation performed upon personal data.

Privileged information - data, which constitute privileged communication.

Sensitive personal information - personal information about:

1. race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. health, education, genetic or sexual life of a person, or any proceeding for any offense, its disposal or the court sentence;
3. issued by government agencies peculiar to an individual (Gov't ID no.); and
4. anything established by law or EO as classified info.

Scope

The law applies to the processing of all types of personal data and to any person involved in such processing.

"Exceptions":

- Info about government officer or employee.
- Info about government contractor.
- Info relating to discretionary benefit of a financial nature given by the government
- Info processed for journalistic, artistic, literary or research purposes;
- Info necessary for public authorities to carry out their functions.
- Info necessary for banks and other financial institutions to comply with applicable laws
- Info originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, which is being processed in the Philippines.

Extraterritorial Application

This law applies to processing done outside of the Philippines if:

1. The personal data is about a Philippine citizen or a resident; and
2. The entity has an established link to the Philippines.

National Privacy Commission

The NPC is the government agency tasked to administer and implement the DPA.

It is attached to the Department of Information and Communications Technology (DICT).

BAR NOTES: Data Privacy Act of 2012

Data Privacy Principles

general: transparency, legitimate purpose and proportionality

specific:

1. Purpose specification
2. Lawfulness and fairness
3. Data quality
4. Collection limitation
5. Retention limitation
6. Security

Criteria (Legal Bases) for Lawful Processing of Personal Info

1. Consent of the DS
2. Contract
3. Legal obligation to which the PIC is subject
4. Protection of vitally important interests of DS
5. National emergency, public order and safety, or functions of public authority
6. Legitimate interests of the PIC or a third party recipient

Criteria (Legal Bases) for Lawful Processing of Sensitive Personal Information and Privileged Info

1. Consent
2. Provided for by existing laws and regulations
3. For the protection of life and health of the DS or another person
4. To achieve lawful and noncommercial objectives of public organizations
5. For medical treatment
6. For the protection of lawful rights and interests of persons in court proceedings, or establishment/defense of legal claims, or when provided to government or public authority.

Subcontracting

A PIC may subcontract the processing of personal data but it will be responsible for ensuring that proper safeguards are in place. The PIP must also comply with all the requirements of the DPA.

Rights of the Data Subject

1. To be informed
2. To Reasonable access
3. To rectification
4. To the suspension or blocking (of data processing), or destruction of personal data
5. To damages
6. To data portability

Transmissibility of DS Rights

DS rights may be exercised by authorized representatives (e.g., lawful heirs and assigns).

When DS rights may not be invoked

1. Info used for scientific and statistical research and, no decisions are taken regarding the DS.
2. Processing for purpose of investigations (criminal, administrative or tax liabilities).

Mandatory data breach notification

The PIC must notify the NPC and affected DS when:

1. sensitive personal information or other information that may be used to enable identity fraud are involved
2. reasonably believed to have been acquired by an unauthorized person
3. the unauthorized acquisition is likely to give rise to a real risk of serious harm to DS.

Principle of Accountability

Each PIC is responsible for the personal data under its control or custody, including those transferred to third parties for processing.

Crimes/Punishable Acts

1. Unauthorized Processing
2. Processing for Unauthorized Purposes
3. Unauthorized Access
4. Accessing Due to Negligence
5. Concealment of Security Breaches involving Sensitive Personal Information
6. Malicious Disclosure
7. Unauthorized Disclosure
8. Improper Disposal

Liability (in the case of Juridical Entities)

If the offender is a juridical person, the penalty shall be imposed on the responsible individuals who participated in the commission of the crime or who, or by their gross negligence, allowed it to happen.

Interpretation

Any doubt in the interpretation of any provision shall be liberally interpreted in favor of the rights and interests of the DS.