DATA PROTECTION LAWS OF THE WORLD

Philippines

DLA PIPER

PHILIPPINES

Last modified 29 December 2022

LAW

The Data Privacy Act of 2012 ("**Act**" or "**DPA**") or Republic Act No. 10173, which took effect on 8 September 2012, is the governing law on data privacy matters in the Philippines.

In 2022, two bills (House Bill No. 892 and House Bill No. 898) were filed in the House of Representatives of the Philippines, seeking to amend the DPA. The proposed amendments under House Bill No. 892 broadly include:

- Increasing the penalties (both the period of imprisonment and monetary fines) for violations of the DPA; and
- Providing for perpetual absolute disqualification as a penalty for a public official or employee who violates provisions of the DPA.

On the other hand, the proposed amendments under House Bill No. 898 broadly include:

- Defining biometric and genetic data.
- Expanding the exclusions on the applicability of the DPA.
- Redefining "sensitive personal information" to include biometric and genetic data, and labor affiliation. Clarifying the extraterritorial application of the DPA by specifying clear instances when the processing of personal data of Philippine citizens and / or residents is concerned.
- Defining the digital age of consent to process personal information as more than fifteen (15) years, applicable where information society services are provided and offered directly to a child.
- Including the performance of a contract as a new criterion of the lawful basis for processing of sensitive personal information.
- Allowing Personal Information Controllers ("**PIC**") outside of the Philippines to authorize Personal Information Processors ("**PIP**") or any other third party in the country, in writing, to report data breaches to the National Privacy Commission ("**NPC**") on behalf of the PIC.
- Modifying criminal penalties under the DPA, giving the proper courts the option to impose either imprisonment or fine upon its sound judgment.

The said bill remains pending before the Philippine House of Representatives.

A further bill was filed in 2022 and is pending before the Philippine Senate (Senate No. 1367) likewise seeking to amend the DPA. Specifically, the bill seeks to exclude the applicability of the DPA to personal information and sensitive personal information that are necessary to address a health crisis during a period of a declared national emergency or pandemic.

Given the rigorous process of passing a law in the Philippines there are no indications that any of these pending bills will be passed into law within the next 12 months.

DEFINITIONS

Definition of personal information

Personal Information is defined in the Act as 'any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.'

The Act, in addition to defining 'Personal Information' that is covered by the law, also expressly excludes certain information from its coverage. These are:

- information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
  - the fact that the individual is or was an officer or employee of the government institution
  - the title, business address and office telephone number of the individual
  - the classification, salary range and responsibilities of the position held by the individual, and
  - the name of the individual on a document prepared by the individual in the course of employment with the government.
- information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services
- information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit
- personal information processed for journalistic, artistic, literary or research purposes (intended for a public benefit)
- information necessary in order to carry out the functions of a public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act ("**CISA**").
- information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or *Bangko Sentral ng Pilipinas* to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws, and
- personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

Definition of sensitive personal information

"Sensitive personal information" is defined in the Act as personal information:

- about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations
- about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offence committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns, and specifically established by an executive order or an act of Congress to be kept classified.

NATIONAL DATA PROTECTION AUTHORITY

The National Privacy Commission ("**NPC**" or **Commission**) is an independent body mandated to administer and implement the Act, and to monitor and ensure compliance of the country with international standards set for personal data protection. The NPC was created in 2016 and the implementing rules and regulations of the Act took effect in the same year.

REGISTRATION

Data Protection Officer

Entities in the Philippines that are engaged in the processing of personal data of individuals residing within and outside the Philippines shall appoint a Data Protection Officer ("**DPO**"). The DPO must be registered with the Commission.

A Certificate of Registration (COR), once issued, shall be valid only until the 8th day of March of the next following year. In view of the global pandemic, the NPC has, on a number of occasions, extended the validity of such CORs. On 4 March 2022, the NPC extended the validity of all existing CORs issued in the year 2021 from 08 March 2022 to 08 March 2023. For CORs issued before 2021, PICs and PIPs must renew their registration with the Commission.

Data Processing Systems

Mandatory registration of data processing systems shall be required from a PIC or PIP if it is processing personal data and operating in the country under any of the following conditions:

- the PIC or PIP employs at least two hundred fifty (250) employees;
- the processing includes sensitive personal information of at least one thousand (1,000) individuals;
- the processing is likely to pose a risk to the rights and freedoms of data subjects. Processing operations that pose a risk to data subjects include those that involve:
    - information that would likely affect national security, public safety, public order, or public health;
    - information required by applicable laws or rules to be confidential;
    - vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a PIC or PIP;
    - automated decision-making; or
    - profiling;
- the processing is not occasional: Provided, that processing shall be considered occasional if it is only incidental to the mandate or function of the PIC or PIP, or, it only occurs under specific circumstances and is not regularly performed. Processing that constitutes a core activity of a PIC or PIP, or is integral thereto, will not be considered occasional: In determining the existence of the foregoing conditions, relevant factors, such as the number of employees, or the records of individuals whose sensitive personal information are being processed, shall only be considered if they are physically located in the Philippines. Data processing systems that involve automated decision-making shall, in all instances, be registered with the NPC. For all other data processing systems whereby the processing is likely to pose a risk to the rights and freedoms of data subjects and is not occasional (as discussed above), the Commission shall determine the specific sectors, industries, or entities that shall be covered by mandatory registration.

The initial list of such sectors, industries, or entities, may be found here.

This list shall be regularly reviewed and may be updated by the NPC through subsequent issuances.

The NPC released a draft circular governing the registration of data processing systems and DPOs, notification regarding automated decision-making or profiling, and the NPC seal of registration. Public consultations on the draft circular were conducted by the NPC in November 2022. As of the date of this update, the NPC has yet to finalize and issue the circular or launch the official registration platform contemplated in the draft circular.

DATA PROTECTION OFFICERS

The PIC of an organization must appoint a person or persons who shall be accountable for the organization's compliance with the Act, and the identity of such person or persons must be disclosed to the data subjects upon the latter's request. The implementing rules and regulations of the Act likewise require any natural or juridical person or other body involved in the processing of personal data to designate an individual or individuals who shall function as DPO, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security. The Act does not specifically provide for the citizenship and residency of the DPO. The Act likewise does not specifically provide for penalties relating to the incorrect appointment of DPOs.

The NPC has published guidelines on the designation of the DPO.

COLLECTION & PROCESSING

The collection and processing of Personal Information must comply with the general principle that Personal Information must be:

- collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;
- processed fairly and lawfully;
- accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;
- adequate and not excessive in relation to the purposes for which they are collected and processed;
- retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed:
    - provided that personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods, and
    - provided, further, that adequate safeguards are guaranteed by said laws authorizing their processing.

In addition, the processing of Personal Information must meet the following criteria, otherwise, such processing becomes prohibited:

- the data subject has given his or her consent;
- the processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- the processing is necessary to protect vitally important interests of the data subject, including life and health;
- the processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
- the processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

The processing of Sensitive Personal Information is prohibited, except in the following cases:

- the data subject has given his or her specific consent prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
- the processing is provided for by existing laws and regulations, provided that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information, and the consent of the data subjects is not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

- the processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
- the processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations, provided:
    - such processing is only confined and related to the bona fide members of these organizations or their associations;
    - the sensitive personal data are not transferred to third parties; and
    - the consent of the data subject was obtained prior to processing.
- the processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
- the processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

TRANSFER

Each PIC is responsible for Personal Information under its control or custody that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

Transfers may involve either data sharing or outsourcing arrangements. "Data sharing" is the disclosure or transfer to a third party of Personal Information under the custody of a PIC or PIP. In the case of the latter, such disclosure or transfer must have been upon the instructions of the PIC concerned. The term excludes "outsourcing," or the disclosure or transfer of personal data by a PIC to a PIP.

Data sharing and outsourcing arrangements must be undertaken in accordance with the requirements under the Act, which includes the execution of the appropriate agreements. The NPC has likewise issued a circular which provides guidelines on data sharing agreements, including the contents thereof.

SECURITY

The personal information controller must implement reasonable and appropriate organizational, physical and technical measures to protect Personal Information against any type of accidental or unlawful destruction, such as from accidental loss, unlawful access, fraudulent misuse, unlawful destruction, alteration, contamination and disclosure, as well as against any other unlawful processing.

The determination of the appropriate level of security must take into account the nature of the Personal Information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation.

In addition, the security measures to be implemented must include the following, which are subject to guidelines that the NPC may issue:

- safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
- a security policy with respect to the processing of personal information;
- a process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

- regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

The personal information controller is obligated to ensure that third parties processing personal information on its behalf shall implement the security measures required by the Act.

The obligation to maintain strict confidentiality of personal information that are not intended for public disclosure extends to the employees, agents or representatives of a personal information controller who are involved in the processing of such personal information.

BREACH NOTIFICATION

The PIC is required to notify both the regulator (which is the NPC) and the affected data subjects within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred.

A security incident is treated as a reportable data breach if Sensitive Personal Information or other information has been acquired by an unauthorized person, and:

- such personal information may, under the circumstances, be used to enable identity fraud; and
- the PIC or the NPC believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

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. The notification shall also include measures taken to reduce the harm or negative consequences of the breach, the representatives of the PIC, including their contact details, from whom the data subject can obtain additional information about the breach, and any assistance to be provided to the affected data subjects.

Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. The NPC may also authorize postponement of notification where such notification may hinder the progress of a criminal investigation related to a serious breach.

Notification is not required if the NPC determines:

- that notification is unwarranted after taking into account compliance by the personal information controller with the Act and the existence of good faith in the acquisition of personal information; or
- in the reasonable judgment of the NPC, such notification would not be in the public interest or in the interests of the affected data subjects.

In April 2022, the NPC launched the Data Breach Notification Management System (DBNMS), an interface that facilitates tracking and submission of personal data breach notifications and annual security incident reports.

ENFORCEMENT

The NPC is responsible for ensuring compliance of the personal information controller with the Act. It has the power to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report. Additionally, the NPC can issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest.

The NPC, however, cannot prosecute violators for breach of the Act for which criminal penalties can be imposed. The Department of Justice is tasked with the prosecution for violations of the Act that are punishable with criminal sanctions.

The following actions are punishable by the Act with imprisonment in varying duration plus a monetary penalty:

- processing of Personal Information or Sensitive Personal Information:
    - without the consent of the data subject or without being authorized by the Act or any existing law; or
    - for purposes not authorized by the data subject or otherwise authorized under the Act or under existing laws;
- providing access to Personal Information or Sensitive Personal Information due to negligence and without being authorized under this Act or any existing law;
- knowingly or negligently disposing, discarding or abandoning the Personal Information or Sensitive Personal Information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection;
- knowingly and unlawfully, or violating data confidentiality and security data systems, breaking in any way into any system where Personal and Sensitive Personal Information is stored;
- concealing the fact of such security breach, whether intentionally or by omission, after having knowledge of a security breach and of the obligation to notify the NPC pursuant to Section 20(f) of the Act;
- disclosing by any personal information controller or personal information processor or any of its officials, employees or agents, to a third party Personal Information or Sensitive Personal Information without the consent of the data subject and without malice or bad faith; and
- disclosing, with malice or in bad faith, by any personal information controller or personal information processor or any of its officials, employees or agents of unwarranted or false information relative to any Personal Information or Sensitive Personal Information obtained by him or her.

In August 2022, the NPC issued a Circular on Administrative Fines for data privacy infractions committed by PICs and PIPs.

ELECTRONIC MARKETING

In 2008, the Department of Trade and Industry, the Department of Health, and the Department of Agriculture issued a joint administrative order implementing the Consumer Act of the Philippines (Republic Act No. 7394) and the E-Commerce Act (Republic Act No. 8792). The Joint DTI-DOH-DA Administrative Order No. 01 (the 'Administrative Order') provides rules and regulations protecting consumers during online transactions, particularly on the purchase of products and services. It covers both local and foreign-based retailers and sellers engaged in e-commerce.

The Administrative Order particularly requires retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce with consumers to refrain from engaging in any false, deceptive and misleading advertisement prohibited under the provisions of the Consumer Act of the Philippines.

In line with the Administrative Order's provision on fair marketing and advertising practices, retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce are mandated to provide:

- fair, accurate, clear and easily accessible information describing the products or services offered for sale such as the nature, quality and quantity thereof;

- fair, accurate, clear and easily accessible information sufficient to enable consumers to make an informed decision whether or not to enter into the transaction; and

- such information that allows consumers to maintain an adequate record of the information about the products and services offered for sale.

A data subject must be provided with specific information regarding the processing of his personal data for direct marketing. In fact, the data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing.

In 2022, the NPC, together with other government agencies, issued Joint Administrative Order No. 2022-01 or the Guidelines for Online Businesses Reiterating the Laws and Regulations Applicable to Online Businesses and Consumers (the "**Guidelines**"). The Guidelines define the responsibilities of online sellers, merchants, or e-retailers under the Act, and seeks to ensure privacy protection and transparency, legitimate purpose and proportionality in data collection and processing.

ONLINE PRIVACY

The Cybercrime Prevention Act of 2012 ("CPA") is the first law in the Philippines which specifically criminalizes computer crimes. The law aims to address legal issues concerning online interactions. The CPA does not define nor does it particularly refer to online privacy, however, it penalizes acts that violate an individual's rights to online privacy, particularly those interferences against the confidentiality, integrity and availability of computer data and systems.

Section 4(c)(3) of the CPA, which provides that unsolicited commercial communications is generally a cybercrime offense punishable under the CPA, was struck down by the Supreme Court for violating the constitutionally guaranteed freedom of expression.

All data to be collected or seized or disclosed will require a court warrant. The court warrant shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce showing that there are:

- reasonable grounds to believe that any of the crimes penalized by the CPA has been committed, or is being committed, or is about to be committed;
- reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and
- no other means readily available for obtaining such evidence.

The integrity of traffic data shall be preserved for a minimum period of six months from the date of the transaction.

Courts may issue a warrant for the disclosure of traffic data if such disclosure is necessary and relevant for the purposes of investigation in relation to a valid complaint officially docketed.

No law in this jurisdiction currently deals with the subject of location data.

Philippine law, including the Act, presently do not define the term "cookies" nor regulate their use. The NPC, however, has opined that cookies, when combined with other pieces of information, may allow an individual to be distinguished from others and may, therefore, be considered as Personal Information. To the extent that cookies are considered as Personal information, the Act may be applicable and consent of the data subjects must be secured prior to (or as soon as practicable and reasonable) the collection and processing of Personal Information, subject to certain exceptions.

KEY CONTACTS

Romulo Mabanta Buenaventura Sayoc & De Los Angeles
www.romulo.com/

Catherine Beatrice O. King Kay
Partner
Romulo Mabanta Buenaventura Sayoc & De Los Angeles
T +63 2 8555 9555
Catherine.Kingkay@romulo.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.