Asia-Pacific
Economic Cooperation

Information Privacy Individual Action Plan
Philippines (2024)

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
A	Is privacy a constitutionally protected right in your economy?	The 1987 Constitution of the Republic of the Philippines https://www.officialgazette.gov.ph/constitutions/1987-constitution/	Article II – Declaration of Policy Section 5. The maintenance peace and order, the protection of life, liberty and property, and the promotion of the general welfare and essential for the enjoyment by all the people of the blessings of democracy. SECTION 11. The State values the dignity of every human person and guarantees full respect for human rights. Section 28. Subject to reasonable conditions prescribed by law, the State adopts and implements a policy of full public disclosure of all its transactions involving public interest.	Article III - Bill of Rights Section 3. (1) xxx (2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.	Implemented

[1] Note here the legislation, rule, code, framework or other privacy protection scheme. Where possible please provide the URL for the website where the legislation or arrangement is available.
[2] Insert the full text or summary of the provisions of your privacy protection scheme(s) that correspond to the APEC Privacy Principles identified in the column titled "APEC Principle/ Commentary".
[3] Sanctions should include the nature of the remedies available, the means by which they are obtained, and by whom (for example, government, local law enforcement, private right of action, etc.).
[4] Identify areas where the practice and the intent of the principle need further consideration; and identify the status of the economies' practice, for example enacted, introduced, draft. If your legislation, rule, code, framework or other privacy protection scheme is at the drafting or proposal stage and has not yet been enacted or implemented, please indicate here and provide any other useful comments."

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			Article III - Bill of Rights Section 1. No person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws. Section 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searchers and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall be issued except upon probable cause to determined personally by the judge after examination under oath or affirmation of the complainant and the witness he may produce, and particularly describing the place to be searched and the persons or things to be seized. Section 3. The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law. Section7. The right of the people to information on matters of public concern shall be recognized. Access to official records, and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for police development, shall be afforded the citizen, subject to such limitations as may be provided by law.		
B			The Data Privacy Act of 2012 (1) protects the privacy of individuals while ensuring	The National Privacy Commission (NPC) is an independent body mandated to	Implemented

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	If not, what other available legislation deals with privacy or confidentiality of personal information.	On 15 August 2012, Republic Act No. 10173 "An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes," also known as the "Data Privacy Act of 2012" was passed into law. This law is the first law on data privacy promulgated in the Philippines. It also created the National Privacy Commission (NPC) which monitors and ensures the protection of the rights of data subjects. The NPC, among its functions, creates Circulars and Advisories for the guidance of the public on different matters relating to privacy and data protection. Available at: https://www.privacy.gov.ph/data-privacy-act/	free flow of information to promote innovation and growth; (2) regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data; and (3) ensures that the Philippines complies with international standards set for data protection through National Privacy Commission. Section 4 of the Data Privacy Act (DPA), which sets out the scope of the law, provides that it applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.	administer and implement the DPA, and to monitor and ensure compliance of the country with international standards set for data protection. Section 7 of the DPA provides for the functions of the NPC which includes: (a) Ensure compliance of personal information controllers with the provisions of this Act; (b) 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: Provided, That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act; xxx	
1	***I Preventing Harm*** **(Ref. Para. 14)** Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent	Data Privacy Act of 2012 https://www.privacy.gov.ph/data-privacy-act/	SEC. 20. Security of Personal Information. – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction,	The DPA provides for penalties for the following offenses: • Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information.	Implemented

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.		alteration and disclosure, as well as against any other unlawful processing. (b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. (c) The determination of the appropriate level of security under this section 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. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include: (1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability; (2) A security policy with respect to the processing of personal information; (3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security	• Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. • Section 27. Improper Disposal of Personal Information and Sensitive Personal Information. • Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. • Section 29. Unauthorized Access or Intentional Breach. • Section 30. Concealment of Security Breaches Involving Sensitive Personal Information. • Section 31. Malicious Disclosure. • Section 32. Unauthorized Disclosure. Pursuant to the authority vested in the National Privacy Commission through Section 7(b) of the Data Privacy Act of 2012 to receive complaints and institute investigations on matters affecting any personal information, the Amendments to Certain Provisions of the the Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission further elaborates on the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.	

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			incidents that can lead to a security breach; and (4) 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. (d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision. (e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations. (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious		

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			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. 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. (1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information. (2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects. (3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.		
		NPC Circular No. 20-02 - RULES ON THE ISSUANCE OF CEASE AND DESIST ORDERS Available at: https://www.privacy.gov.ph/wp-content/uploads/2020/10/NPC-Circular-20-02_Circular-Rules-on-CDO.pdf	Section 4. Grounds for the Issuance of Cease and Desist Order. – No CDO shall be issued unless it is established by substantial evidence that all of the following concur: A. the Adverse Party is doing, threatening or is about to do, is procuring to be done,		

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
		NPC Circular 20-01 – Guidelines on the Processing of Personal Data for Loan-Related Transactions Available at: https://www.privacy.gov.ph/wp-content/uploads/2020/10/NPC-Circular-No.-20-01.pdf	some act or practice in violation of the DPA, its IRR, or other related issuances; B. such act or practice is detrimental to national security or public interest, or the CDO is necessary to preserve and protect the rights of a data subject; and C. the commission or continuance of such act or practice, unless restrained, will cause grave and irreparable injury to a data subject. SECTION 3. Guidelines. — The processing of personal data for evaluating loan applications, granting loans, collection of loans, and closure of loan accounts shall be subject to the following general guidelines: A. Borrowers shall be provided all the details required under Section 16 (b) of the DPA and Section 34 (a)(2) of its IRR, in a clear language and in the most appropriate format. X x x B. In cases where a borrower's personal data will be further processed for purposes compatible with the primary purpose, the same may be allowed, provided that: x x x C. LCs, FCs, and other persons acting as such shall limit the collection of personal data from the borrowers to those which are adequate, relevant, suitable, necessary, and not excessive in relation with the applicable know your customer (KYC) policies, rules and regulations, as well as those necessary for determining		

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			creditworthiness and preventing fraud. X x x D. Where online apps are used for loan processing activities, LCs, FCs, and other persons acting as such shall be prohibited from requiring unnecessary permissions that involve personal and sensitive personal information. X x x E. LCs, FCs, and other persons acting as such shall bear in mind that they are at all times accountable for personal data under its control or custody. They shall not use any personal data to engage in unfair collection practices as defined under SEC Memorandum Circular No. 18 series of 2019. Such practices may also be construed as a punishable act under the DPA; and F. LCs, FCs, and other persons acting as such shall adopt and implement reasonable policies regarding the retention of the personal data of those whose loan applications were denied and of borrowers who have fully settled their loans. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined. Otherwise, applicable penalties as provided for in the DPA may be imposed.		

2	***II Notice*** **(Ref. Para. 15-17)** Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: a) the fact that personal information is being collected; b) the purposes for which personal information is collected; c) the types of persons or organizations to whom personal information might be disclosed; d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information. All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such	Data Privacy Act of 2012	SEC. 11. General Data Privacy Principles. – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. xxx SEC. 16. Rights of the Data Subject. – The data subject is entitled to: (a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed; (b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: (1) Description of the personal information to be entered into the system; (2) Purposes for which they are being or are to be processed; (3) Scope and method of the personal information processing; (4) The recipients or classes of recipients to whom they are or may be disclosed; (5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;	The DPA provides for penalties for the following offenses: • Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. • Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. • Section 27. Improper Disposal of Personal Information and Sensitive Personal Information. • Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. • Section 29. Unauthorized Access or Intentional Breach. • Section 30. Concealment of Security Breaches Involving Sensitive Personal Information. • Section 31. Malicious Disclosure. • Section 32. Unauthorized Disclosure Pursuant to the authority vested in the National Privacy Commission through Section 7(b) of the Data Privacy Act of 2012 to receive complaints and institute investigations on matters affecting any personal information, the Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission further elaborates on the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.	Implemented

	notice should be provided as soon after as is practicable. It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information.		(6) The identity and contact details of the personal information controller or its representative; (7) The period for which the information will be stored; and (8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission. Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: Provided, That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation; xxx		

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
3	***III Collection Limitation*** **(Ref. Para. 18)** The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.	Data Privacy Act of 2012	SEC. 11. General Data Privacy Principles. – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Personal information must, be:, (a) 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; (b) Processed fairly and lawfully; xxx SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: (a) The data subject has given his or her consent; xxx SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:	The DPA provides for penalties for the following offenses: • Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. • Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. • Section 27. Improper Disposal of Personal Information and Sensitive Personal Information. • Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. • Section 29. Unauthorized Access or Intentional Breach. • Section 30. Concealment of Security Breaches Involving Sensitive Personal Information. • Section 31. Malicious Disclosure. • Section 32. Unauthorized Disclosure Pursuant to the authority vested in the National Privacy Commission through Section 7(b) of the Data Privacy Act of 2012 to receive complaints and institute investigations on matters affecting any personal information, the Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission further elaborates on the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.	Implemented

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			(a) The data subject has given his or her consent x x x.		
4	***IV Use of Personal Information*** **(Ref. Para. 19)** Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.	Data Privacy Act of 2012	SEC. 11. General Data Privacy Principles. – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. xxx SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: (a) The data subject has given his or her consent; (b) 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 DPA provides for penalties for the following offenses: • Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. • Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. • Section 27. Improper Disposal of Personal Information and Sensitive Personal Information. • Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. • Section 29. Unauthorized Access or Intentional Breach. • Section 30. Concealment of Security Breaches Involving Sensitive Personal Information. • Section 31. Malicious Disclosure. • Section 32. Unauthorized Disclosure	Implemented

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject; (d) The processing is necessary to protect vitally important interests of the data subject, including life and health; (e) 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 (f) 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. SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;	Pursuant to the authority vested in the National Privacy Commission through Section 7(b) of the Data Privacy Act of 2012 to receive complaints and institute investigations on matters affecting any personal information, the Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission further elaborates on the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.	

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			(b) The processing of the same 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: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information; (c) 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; (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing; (e) 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 (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of		

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.		

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
5	***V Choice*** **(Ref. Para. 20)** Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.	Data Privacy Act of 2012	Under Sections 12 and 13 of the DPA, Consent of the data subject is one of the bases for lawful processing of personal information and sensitive personal information. Section 3 of the DPA defines Consent of the data subject as any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.	The DPA provides for penalties for the following offenses: • Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. • Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. • Section 27. Improper Disposal of Personal Information and Sensitive Personal Information. • Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. • Section 29. Unauthorized Access or Intentional Breach. • Section 30. Concealment of Security Breaches Involving Sensitive Personal Information. • Section 31. Malicious Disclosure. • Section 32. Unauthorized Disclosure The Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission further elaborates on the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.	Implemented

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
6	***VI Integrity of Personal Information*** **(Ref. Para. 21)** Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.	Data Privacy Act of 2012	SEC. 11. General Data Privacy Principles. – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Personal information must, be:, xxx (c) 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;	The DPA provides for penalties for the following offenses: • Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. • Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. • Section 27. Improper Disposal of Personal Information and Sensitive Personal Information. • Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. • Section 29. Unauthorized Access or Intentional Breach. • Section 30. Concealment of Security Breaches Involving Sensitive Personal Information. • Section 31. Malicious Disclosure. • Section 32. Unauthorized Disclosure The Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission further elaborates on the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.	Implemented

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
7	***VII Security Safeguards*** **(Ref. Para. 22)** Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.	Data Privacy Act of 2012	SEC. 20. Security of Personal Information. – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. (b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. (c) The determination of the appropriate level of security under this section 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. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include: (1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability; (2) A security policy with respect to the processing of personal information;	The DPA provides for penalties for the following offenses: • Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. • Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. • Section 27. Improper Disposal of Personal Information and Sensitive Personal Information. • Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. • Section 29. Unauthorized Access or Intentional Breach. • Section 30. Concealment of Security Breaches Involving Sensitive Personal Information. • Section 31. Malicious Disclosure. • Section 32. Unauthorized Disclosure The Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission further elaborates on the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.	Implemented

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			(3) 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 (4) 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. (d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision. (e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations. (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable		

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat 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. 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. (1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information. (2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects. (3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach. Sections 22 to 24 of the DPA include provisions specific to security of sensitive personal information in the government.		

8	***VIII Access and Correction*** **(Ref. Para. 23-25)** Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; iv. in a form that is generally understandable; and, c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted. Such access and opportunity for correction should be provided except where: (i) the burden or expense of doing so would be unreasonable or	Data Privacy Act of 2012	SEC. 16. Rights of the Data Subject. – The data subject is entitled to: xxx (c) Reasonable access to, upon demand, the following: (1) Contents of his or her personal information that were processed; (2) Sources from which personal information were obtained; (3) Names and addresses of recipients of the personal information; (4) Manner by which such data were processed; (5) Reasons for the disclosure of the personal information to recipients; (6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject; (7) Date when his or her personal information concerning the data subject were last accessed and modified; and (8) The designation, or name or identity and address of the personal information controller; (d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal	Section 16(f) of the DPA provides that data subjects may be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information. The DPA provides for penalties for the following offenses: • Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. • Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. • Section 27. Improper Disposal of Personal Information and Sensitive Personal Information. • Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. • Section 29. Unauthorized Access or Intentional Breach. • Section 30. Concealment of Security Breaches Involving Sensitive Personal Information. • Section 31. Malicious Disclosure. • Section 32. Unauthorized Disclosure The Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission further elaborates on the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.	Implemented

	disproportionate to the risks to the individual's privacy in the case in question; (ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or (iii) the information privacy of persons other than the individual would be violated. If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.	*NPC Advisory No. 2021-01 - Data Subject Rights* Available at: https://www.privacy.gov.ph/wp-content/uploads/2021/02/NPC-Advisory-2021-01-FINAL.pdf	information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: Provided, That the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject; Xxx SECTION 3. Exercise of rights. — These rights shall be exercised by the data subject himself or herself. The data subject may, however, authorize another person to facilitate the exercise of any of these rights on his or her behalf: provided, that the authorization is specific and supported by appropriate documents. SECTION 4. Transmissibility of rights. — The lawful heirs and assigns of the data subject may likewise exercise any of his or her rights, at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the same. SECTION 5. Policies and procedures. — PICs shall establish policies and procedures allowing for the exercise of data subjects of their rights. The following shall be considered: x x x SECTION 8. Right to Access. — The right of data subjects to access information on the processing of their personal data shall be subject to the following guidelines: x x x SECTION 9. Right to Rectification. — The data subject has the right to dispute the	Pursuant to the authority vested in the National Privacy Commission through Section 7(b) of the Data Privacy Act of 2012 to receive complaints and institute investigations on matters affecting any personal information, the Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission further elaborates on the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.	

			inaccuracy or error in his or her personal data and have the PIC correct the same within a reasonable period of time. x x x		

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
9	***IX Accountability*** **(Ref. Para. 26)** A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.	Data Privacy Act of 2012	SEC. 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. (b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.	The DPA provides for penalties for the following offenses: • Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. • Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. • Section 27. Improper Disposal of Personal Information and Sensitive Personal Information. • Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. • Section 29. Unauthorized Access or Intentional Breach. • Section 30. Concealment of Security Breaches Involving Sensitive Personal Information. • Section 31. Malicious Disclosure. • Section 32. Unauthorized Disclosure Pursuant to the authority vested in the National Privacy Commission through Section 7(b) of the Data Privacy Act of 2012 to receive complaints and institute investigations on matters affecting any personal information, the Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission further elaborates on the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.	Implemented

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
C	Network point of contact arrangements[5]		Contact details will be made available to APEC members through the APEC Secretariat.		

-- // --

[5] *Please provide contact details such as name and/or title, address, telephone and email contacts. This information will not be published but will be made available to economies.*