Asia-Pacific Economic Cooperation

Information Privacy Individual Action Plan (Template Revised 2016)

Singapore (submitted 2022)

	APEC Principle / Commentary / Implementation guidance	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?	While privacy is not a constitutionally protected right, related privacy interests are protected in Singapore through a combination of the Personal Data Protection Act ("PDPA") and other laws, such as harassment laws, defamation laws and the laws of confidence. Singapore's Constitution available at: http://statutes.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?&actno=Revd-	N.A.	N.A.	N.A.

[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 / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
		CONST&date=latest&method=part			
B	If not, what other available legislation deals with privacy or confidentiality of personal information.	- The PDPA was promulgated to govern the collection, use and disclosure of personal data by private sector organisations. The PDPA first came into full effect on 2 July 2014, and the most recent amendments to the PDPA came into effect on 1 Feb 2021. The PDPA applies concurrently with the Common Law and other sectoral legislations that may include provisions on the protection of personal data from misuse. This table will primarily cover the provisions within the PDPA. ***PDPA is available at: http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0***	In brief, the Data Protection provisions cover the following: *1. Accountability Obligation* Undertake measures to ensure that organisations meet their obligations under the PDPA such as making information about your data protection policies, practices and complaints process available upon request and designating a data protection officer (DPO) and making the business contact information available to the public. *2. Notification Obligation* Notify individuals of the purposes for which your organisation is intending to collect, use or disclose their personal data. *3. Consent Obligation* Only collect, use or disclose personal data for purposes which an individual has given his/her consent to. Allow the individual to withdraw consent, with reasonable notice, and inform him/her of the likely consequences of withdrawal.	The Commission may give directions to an organisation to ensure its compliance with the Act, and may impose a financial penalty of up to SGD $1M or 10% of an organisation's annual gross turnover in Singapore, whichever is higher. Such directions may be enforced through the courts. Any person who suffers loss or damage directly as a result of a contravention by an organisation of any Data Protection provision has a right of private action for relief in civil proceedings in a court. (See Parts IXC and IXD of the Act). Prosecution of offences is available in relation to specified offences, e.g. making an access or correction request relating to the personal data of another individual with the authorization of that individual. Persons found guilty of such offences may be liable to a fine and/or imprisonment. (See, for example, Section 51 of the Act.)	Enacted

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			Once consent is withdrawn, make sure that you cease to collect, use or disclose the individual's personal data. *4. Purpose Limitation Obligation* Only collect, use or disclose personal data for the purposes that a reasonable person would consider appropriate under the given circumstances and for which the individual has given consent. An organisation may not, as a condition of providing a product or service, require the individual to consent to the collection, use or disclosure of his or her personal data beyond what is reasonable to provide that product or service. *5. Accuracy Obligation* Make reasonable effort to ensure that the personal data collected is accurate and complete, especially if it is likely to be used to make a decision that affects the individual or to be disclosed to another organisation. *6. Protection Obligation* Reasonable security arrangements have to be made to protect the personal data in your organisation's possession		

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			to prevent unauthorised access, collection, use, disclosure or similar risks. *7. Retention Limitation Obligation* Cease retention of personal data or dispose of it in a proper manner when it is no longer needed for any business or legal purpose. *8. Transfer Limitation Obligation* Transfer personal data to another economy only according to the requirements prescribed under the regulations, to ensure that the standard of protection is comparable to the protection under the PDPA, unless exempted by the PDPC. *9. Access and Correction Obligation* Upon request, organisations have to provide individuals with access to their personal data as well as information about how the data was used or disclosed within a year before the request. Organisations are also required to correct any error or omission in an individual's personal data as soon as practicable and send the corrected data to other organisations to which the		

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			personal data was disclosed (or to selected organisations that the individual has consented to), within a year before the correction is made. *10. Data Breach Notification Obligation* In the event of a data breach, organisations must take steps to assess if it is notifiable. If the data breach likely results in significant harm to individuals, and/or are of significant scale, organisations are required to notify the PDPC and the affected individuals as soon as practicable. 11. Data Portability Obligation (not brought into force yet) At the request of the individual, organisations are required to transmit the individuals' data that is in the organisation's possession or under its control, to another organization in a commonly used machine-readable format. (Some of the matters mentioned above may have other related requirements which organisations must comply with. In addition, some of abovementioned matters are		

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			subject to exceptions or limitations specified in the PDPA.) The data protection provisions in the PDPA do not impose obligations on individuals acting in a personal or domestic capacity, employees, and public agencies.		
1	***I Preventing Harm*** **(Ref. Para. 20)** Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent 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.	PDPA This principle is not explicitly acknowledged in PDPA, but preventing misuse is one of the key objectives of the PDPA.	To protect the personal data of individuals, generally speaking, the PDPA outlines 10 main obligations for organisations that collect, use and disclose personal data to comply with. The 11 main obligations are: i. Accountability Obligation ii. Consent Obligation iii. Purpose Limitation Obligation iv. Notification Obligation v. Access and Correction Obligation vi. Accuracy Obligation vii. Protection Obligation viii. Retention Limitation Obligation ix. Transfer Limitation Obligation x. Data Breach Notification Obligation	N.A.	Enacted

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			xi. Data Portability Obligation (not brought into force yet) For example, the sensitivity of personal information collected is a consideration in deciding the nature and extent of security safeguards to apply to data collected for compliance with Section 24 of the PDPA.		
2	***II Notice*** **(Ref. Para. 21-23)** 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;	PDPA	Section 11 – Accountability Obligation An organization shall designate one or more individuals to be responsible for ensuring that the organization complies with the PDPA. Organisation shall make available to the public the business contact information of at least one of these individuals. Organisation shall also develop, implement and make available on request about policies and practices that are necessary for the organization to meet the obligations of the organization under the PDPA. Section 20 - Notification Obligation Organisations should notify individuals of the purposes for which the organisations are	See (B) above	See (B) above

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	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 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.		intending to collect, use or disclose their personal data on or before such collection, use or disclosure of personal data. However, organisations are not required to provide notifications of the purposes in certain circumstances set out in the PDPA, which includes where the personal data is publicly available. Section 18 - Purpose Limitation Obligation Organisations may collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent. Organisations may not, as a condition of providing a product or service, require the individual to consent to the collection, use or disclosure of his or her personal data beyond what is reasonable to provide that product or service.		
3	***III Collection Limitation*** **(Ref. Para. 24)**	PDPA	Section 14 & 18 - Purpose Limitation Obligation and Consent Obligation	See (B) above	See (B) above

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	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.		Organisations may collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has been notified and given consent. Organisations may not, as a condition of providing a product or service, require the individual to consent to the collection, use or disclosure of his or her personal data beyond what is reasonable to provide that product or service. Any consent given in such circumstances is not valid for purposes of the PDPA. Section 4(6), Section 13 & Section 17 – The organisation need not notify the purposes and/or obtain the consent of the individual in certain circumstances set out in the PDPA.		
4	***IV Use of Personal Information*** **(Ref. Para. 25)** Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:	PDPA	Section 14 & 18 - Purpose Limitation Obligation and Consent Obligation Organisations may collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances. and for which	See (B) above An individual who makes use of personal data in the possession or under the control of an organization or a public agency, and the use is not authorized by the organization or public agency (knowing or reckless), shall be liable of an offence and	See (B) above

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	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.		the individual been notified and has given consent. Organisations may not, as a condition of providing a product or service, require the individual to consent to the collection, use or disclosure of his or her personal data beyond what is reasonable to provide that product or service. Any consent given in such circumstances is not valid for purposes of the PDPA. Section 4(6), Section 13 & Section 17 – The organisation need not notify the purposes and/or obtain the consent of the individual in certain circumstances set out in the PDPA. This includes not having to obtain consent where the collection, use or disclosure (as the case may be) without consent is required or authorized under other written law.	shall be liable on conviction to a fine not exceeding $5000 or to imprisonment for a term not exceeding 2 years or to both.	
5	***V Choice*** **(Ref. Para. 26)** Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the	PDPA	Section 13 and Section 16 - Consent Obligation and Withdrawal of Consent Only collect, use or disclose personal data for purposes for which an individual has given his or her consent. Allow individuals to withdraw consent at anytime, with reasonable	See (B) above	See (B) above

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	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.		notice, and inform them of the likely consequences of withdrawal. Upon withdrawal of consent to the collection, use or disclosure for any purpose, your organization (and cause its data intermediaries and agents) to cease such collection, use or disclosure of the personal data. The foregoing is subject to any collection, use or disclosure without consent that is required or authorized under the PDPA or other written law. One of the exceptions to the requirement for consent for collection, use and disclosure of personal data is in situations when the personal data is publicly available. (Exception for publicly available personal data can be found in the First Schedule, Part 2 of the PDPA)		
6	***VI Integrity of Personal Information*** **(Ref. Para. 27)** Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.	PDPA	Section 23 - Accuracy Obligation Organisations shall make reasonable effort to ensure that personal data collected by or on behalf of their organisations are accurate and complete, if it is likely to be used to make a decision that affects the individual, or if it is likely to be	See (B) above	See (B) above

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			disclosed to another organisation.		
7	***VII Security Safeguards*** **(Ref. Para. 28)** 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.	PDPA	**Section 24 -** 6. Protection Obligation Organisations shall make reasonable security arrangements to protect the personal data that their organisations possess or control to prevent (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks (b) the loss of any storage medium or device on which personal data is stored. .	See (B) above	See (B) above
8	***VIII Access and Correction*** **(Ref. Para. 29-31)** Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal	PDPA	**Sections 21 and 22 – Access and Correction Obligations** Upon request, the personal data of an individual and information about the ways in which his or her personal data has been or may have been used or disclosed within a year before the request should be provided.	See (B) above Specifically in respect of access and correction, on the application of a complainant, the Commission may review a refusal to provide access or make a correction or a failure to provide access or make the correction within a reasonable	See (B) above

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	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 disproportionate to the risks to the individual's privacy in the case in question;		In certain circumstances set out in the PDPA, access is prohibited (see Section 21(3)) or access need not be provided (see, in particular, Section 21(2) read with Fifth Schedule to the PDPA.) Organisations are also required to correct any error or omission in an individual's personal data upon his or her request. Unless the organisations are satisfied on reasonable grounds that the correction should not be made, the organisations should correct the personal data as soon as practicable and send the corrected data to other organisations to which the personal data was disclosed within a year before the correction is made (or for organisations other than credit bureaus, with the individual's consent, only to selected organisations). In certain circumstances set out in the PDPA, correction need not be made (see, in particular, Section 22(6), (7) and the Sixth Schedule to the PDPA.) You may also wish to refer to Part II of the Personal Data Protection Regulations 2021.	time, or a fee required from the complainant in relation to an access or correction request. Upon completion of its review, the Commission may: (a) confirm the refusal to provide access to the personal data, or direct the organisation to provide access to the personal data, within a specified time; (b) confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant; or (c) confirm the refusal to correct the personal data, or direct the organisation to correct the personal data, in a specified manner and time. (See Section 48H of the Act.)	

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	(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.				
9	***IX Accountability*** **(Ref. Para. 32)** 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	PDPA	**Section 11 – Accountability Obligation** Organisations are responsible for personal data in its possession or under its control and shall designate one or more individuals to be responsible for ensuring compliance with the Act. **Section 14 & 18 - Purpose Limitation Obligation and Consent Obligation** Organisations may disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual been notified and has	See (B) above	See (B) above

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	person or organization will protect the information consistently with these Principles.		given consent. (Except that the organisation need not notify the purposes and/or obtain the consent of the individual in certain circumstances set out in the PDPA.) **Section 26 Transfer Limitation Obligation –** An organisation may only transfer personal data out of Singapore in accordance with requirements prescribed under the PDPA to ensure that the organisations overseas provide a standard of protection to the personal data so transferred that is comparable to the protection under the PDPA. You may also wish to also refer to Part III of the Personal Data Protection Regulations 2021.		
C	**Domestic Implementation**				
	Giving Effect to the Framework - Establishment of a Privacy Enforcement Authority **(Ref. Para. 41)** Member Economies should consider establishing and maintaining Privacy Enforcement Authorities which are provided with the governance, resources and technical expertise necessary to exercise their powers effectively and to	PDPA	**Sections 5 and 6 – Personal Data Protection Commission and Functions of Commission** The Info-communications Media Development Authority is designated as the Personal Data Protection Commission (PDPC). The PDPC is responsible for the administration of the Personal Data Protection Commission.	See (B) above	See (B) above

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	make decisions on an objective, impartial and consistent basis.		The functions of the Commission shall be to promote awareness of data protection in Singapore, to provide consultancy, advisory, technical, managerial or other specialist services relating to data protection, to advise the Government on all matters relating to data protecton, etc.		
	Privacy Management Programmes **(Ref. Para. 44)** Member Economies should consider encouraging personal information controllers to implement privacy management programmes that: (i) are tailored to the structure and scale of their operations, and the volume and sensitivity of the personal information under their control; (ii) provide appropriate safeguards based on risk assessment that takes into account the potential harm to individuals; (iii) are integrated into accountable governance structures with	Data Protection Management Programme	**<u>Data Privacy Management Programme (DPMP)</u>** The DPMP is a four-step programme to help organisations establish a robust data protection infrastructure. The DPMP is encouraged but not mandatory. (i) Establishing a governance structure to define values and identify risks with organizational leadership. o The way in which an organization collects, uses, discloses and stores personal data is documented using diagrams and charts so that risks can be identified at every stage of the data lifecycle. o The risks are rated according to the impact and likelihood of occurring.	N.A.	N.A.

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	appropriately trained personnel and establish internal oversight mechanisms; (iv) include mechanisms for responding to inquiries and incidents; (v) are updated in light of ongoing monitoring and periodic assessment.		o A risk management strategy with appropriate technical, administrative and physical controls to be implemented. (ii) Developing a data protection policy and designating data protection roles and responsibilities of the staffs in organisation o Data protection policy could include data protection notices, consent clauses in contracts/forms, acceptable use policy, third party contracts, etc. o Data Protection Officer is appointed from the Senior Management to oversee all personal data protection related matters, and liases with each department representative. (iii) Designing processes to operationalize policy o Confidentiality or non-disclosure agreement concerning personal and proprietary information to be signed by all employees; PDPA clauses included in employment contracts.		

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			(iv) Detailing steps to keep data protection policies and processes up-to-date o Data protection policies are regularly reviewed and amended through general feedback, international trends and best practices, enforcement decisions by the PDPC, after data incidents, whenever business changes, etc.		
	Promotion of Technical Measures to Protect Privacy **(Ref. Para. 46)** When considering approaches to give effect to the Framework, Member Economies should promote technical measures which help to protect privacy.	Generally, we have tools such as Advisory Guidelines, Sample Templates and Certifications that help companies to adopt technical measures which help to protect privacy. E.g. Data Privacy Management Programme (DPMP), Guide to Data Protection for ICT systems For further information, please visit our website www.pdpc.gov.sg/Help-and-Resources	**Data Privacy Management Programme (DPMP)** Organisations are encouraged to minimize the likelihood of the risk occurring and impact if it does occur. Technical controls use technology as a basis for controlling the access to and usage of personal and sensitive data in IT systems and over computer networks e.g,encryption, 2-factor authentication. **Guide to Data Protection Practices for ICT systems** The data protection practices for ICT systems are grouped into three main sections – (1) Policy/Risk Management for ICT systems, (2) ICT controls and (3) SOP/IT operations. Each section recommends the basic and enhanced ICT practices that organisations can put in place to	N.A.	N.A.

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			support each stage of the data lifecycle.		
	Public Education and Communication **(Ref. Para. 48)** Member Economies should: (a) publicise how their Privacy Laws and other domestic arrangements provide privacy protections to individuals; and (b) engage in activities that raise awareness amongst personal information controllers and processors about their responsibilities and obligations.	PDPA	PDPC educates industry their PDPA obligations and consumers of their rights and responsibilities to protect their personal data through a variety of campaigns, outreach programmes and other communication channels, as follows. **<u>Industry</u>** In brief, the PDPC generally educates organisations on their obligations via: **Events** 1. Annual Personal Data Protection Seminar since 2013 2. Privacy Awareness Week seminars and workshops since 2015 3. Industry Briefings through trade associations and chambers since inception **Training** 4. Data Protection (DP) courses rolled out in 2015: (i) Fundamentals of the PDPA and (ii) Practitioner's Certificate in Personal Data Protection Preparatory Course in 2018 5. DP Advisory sessions launched in 2017 6. E-Learning Programme and Assessment as part of organisations' training of	N.A.	**<u>Industry (based on PDPC's 2020 survey)</u>** 88% of organisations in Singapore are aware of the PDPA • 87% agree that it strengthens Singapore's position as a trusted hub and choice location for data hosting and management activities • 84% agree that it helps prepare organisations for digital economy by facilitating innovative use of data while ensuring a certain standard of protection of data **<u>Consumer (based on PDPC's 2020 survey)</u>** • 76% of individuals in Singapore are

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			staff revamped and launched in 2021 (first version launched in 2014) **Online Channels** 7. DPO Connect e-newsletter since 2015 8. Social media channel LinkedIn since 2014 **<u>Consumer</u>** In brief, PDPC generally reaches out to educate consumers via: 1. Partnership with public agencies and industry partners 2. Roadshows and activity kit with schools since 2014 3. Online data protection games for consumers, with the first launched in 2017 4. Social media channel Facebook since 2014, with addition of Instagram and Telegram in 2021		aware of the PDPA • 88% agree that a data protection law is important in Singapore • 86% feel responsible for the protection of own's personal data
	Cooperation Within and Between Public and Private Sectors **(Ref. Para. 49, 51)** Member Economies should seek the cooperation of non-government stakeholders in furthering the Framework's objectives. Member Economies should consider developing strategies that	PDPA	**PDPA** PDPC work with sector regulators/champions to publish sector-specific materials. So far, PDPC has published seven sector-specific guidelines, including those for the healthcare, real estate and education industry. PDPC has also been working with Trade Associations and Chamber of Commerce (TACs) to engage their members. **Section 4 – Application of Act**	N.A.	N.A.

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	reflect a coordinated approach to implementing privacy protections across governmental bodies.		The PDPA does not cover public agencies. the Data Protection Provisions shall not impose any obligation on any public agency. **Section 10 – Co-operation agreements** For the purposes of Section 59, a cooperation agreement is an agreement for the purposes of facilitating cooperation between the Commission and another regulatory authority in the performance of their respective functions in so fat as those functions relate to data protection and avoiding duplication of activities by the Commission and another regulatory authority surrounding enforcement of data protection laws.		
	Appropriate Remedies where Privacy Protections are Violated **(Ref. Para. 53, 54)** A Member Economy's system of privacy protections should include appropriate remedies for privacy violations, which could include redress, the ability to stop a violation from continuing, and other remedies. Member Economies should consider encouraging or requiring personal	PDPA	**Section 48I – Directions for non-compliance** The Commission may, if it is satisfied that an organization has not complied or is not complying with any provision of Part 3 to 6A, give the organization or person any direction that the Commission thinks fit in the circumstances to ensure compliance with that provision. **Section 26 – Data Breach Notification Obligation** Where an organization assesses that a data breach is a notifiable	See (B) above	See (B) above

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	information controllers to provide notice, as appropriate, to Privacy Enforcement Authorities and/or other relevant authorities in the event of a significant security breach affecting personal information under its control. Where it is reasonable to believe that the breach is likely to affect individuals, timely notification directly to affected individuals should be encouraged or required, where feasible and reasonable.		data breach, the organization must notify the Commission as soon as is practicable but in any case no later than 3 calendar days after the day the organization makes that assessment. Organisations must also notify affected individuals if the data breach is likely to result in significant harm or impact to them (exceptions apply).		
	International Implementation				
	Cross-Border Cooperation in Investigation and Enforcement (Ref. Para.62) Member Economies should expand their use of existing cooperative arrangements and consider developing additional cooperative arrangements or procedures, as necessary, to facilitate cross-border cooperation in the enforcement of privacy laws.	PDPC has in place several Memoranda of Understanding (MOU) with other jurisdictions. Sharing sessions were conducted to share best practices and experiences on data protection policies and regulations, as well as enforcement frameworks and initiatives. Information exchange was also conducted to facilitate investigations. PDPC is also a member of the Global Privacy Enforcement Network (GPEN).	N.A.	N.A.	N.A.

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	Cross-Border Privacy Mechanisms **(Ref. Para. 66)** Member Economies will endeavor to support the development and recognition or acceptance of cross-border privacy mechanisms for use by organisations to transfer personal information across the APEC region, recognizing that organizations would still be responsible for complying with local privacy requirements as well as with all applicable laws.	PDPA recognises various mechanisms under the Transfer Limitation Obligation, including APEC CBPR/ PRP certifications, contracts, binding corporate rules, and other legally binding documents. The Infocomm Media Development Authority also has in place Digital Trade Agreements (DEPA, SADEA etc.) and MOUs to facilitate cross-border data flows with other jurisdictions. The mechanisms include CBPR certification, appropriate recognition of comparable protection afforded by domestic legal frameworks' national trustmark or certification frameworks (E.g., Data Protection Trustmark), ASEAN Model Contractual Clauses etc.	N.A.	N.A.	N.A.
	Cross-Border Transfers **(Ref. Para. 70)** A Member Economy should refrain from restricting cross-border flows of personal information between itself and another Member Economy where: (a) The other Economy has in place legislative or regulatory instruments that give effect to the Framework; or (b) sufficient safeguards exist including effective	PDPC recognises the APEC CBPR and PRP as transfer mechanisms in their own right under the Transfer Limitation Obligation in PDPA. This allows organisations in Singapore to transfer personal data to an overseas recipient that is CBPR- or PRP-certified, without additional requirements. PDPC also recognises the ASEAN Model Contractual Clauses (MCCs) to fulfil the Transfer Limitation Obligation under the PDPA. Businesses may adapt these clauses with appropriate modifications at their discretion for transfers between businesses	N.A.	N.A.	N.A.

	APEC Principle / Commentary / Implementation guidance	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it.	within Singapore, or transfers to jurisdictions outside ASEAN.			
D	**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 Member Economies.*