Annex B[1]

APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS: ENFORCEMENT MAP

As outlined in the Charter of the APEC Cross Border Privacy Rules (CBPR) System's Joint Oversight Panel (JOP), an APEC Member Economy is considered a Participant in the CBPR System after the Chair of the Electronic Commerce Steering Group (ECSG Chair) has notified the Economy that the following conditions have been met:

(i) The Economy's ECSG delegation, or appropriate governmental representative, submits to the ECSG Chair a letter indicating its intention to participate and confirming that at least one Privacy Enforcement Authority in that Economy is a participant in the APEC Cross Border Privacy Enforcement Arrangement (CPEA);

(ii) The Economy indicates its intention to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2 of the Charter of the JOP;

(iii) The Economy's ECSG delegation, or appropriate governmental representative, after consulting with the JOP, submits to the Chair of the ECSG an explanation of how the CBPR System program requirements may be enforced in that Economy; and

(iv) The JOP submits to the Chair of the ECSG a report as to how the conditions in (i)-(iii) above have been satisfied.

The purpose of Annex B is to assist Economies and the JOP in fulfilling the requirements of items (iii) and (iv):

- This document provides the baseline program requirements of the APEC Cross Border Privacy Rules (CBPR) System in order to guide the Economy's explanation of how each requirement may be enforced in that Economy; and

- The information provided by the Economy will form the basis of the JOP's report.

Column 1 lists the questions in the intake questionnaire to be answered by an applicant organization when seeking CBPR certification. Column 2 lists the assessment criteria to be used by an APEC-recognized Accountability Agent when verifying the answers provided in Column 1. Column 3 is for use by the Economy's ECSG delegation or appropriate governmental representative when explaining the enforceability of an applicant organization's answers in Column 1. Accountability Agents should be able to enforce the CBPR program requirements through law or contract and an economy's relevant privacy enforcement authorities should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the

[1] Annex B and the table that follows do not purport to provide a complete and comprehensive account of the PDPC's privacy enforcement authority. It is not intended to be relied on as legal advice and should not be used as statements of law in the context of legal proceedings. In particular, any advisory guidelines and guides cited are not legally binding on PDPC or any other party and do not modify in any way the legal effect and interpretation of any laws.

CBPR program requirements. Additional documentation to assist in these explanations may be submitted as necessary. This document is to be read consistently with the qualifications to the provision of notice, the provision of choice mechanisms, and the provision of access and correction mechanisms found in the CBPR Intake Questionnaire.

NOTICE

Assessment Purpose – *To ensure that individuals understand the applicant's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.*

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible; • Applies to all personal information; whether collected online or offline; • States an effective date of Privacy Statement publication.	**Policies and practices** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[2] and 18(b), an organisation shall inform the individual of –

[2] PDPA Section 14(1): An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	Where Applicant answers **NO** to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15[3]; or

[3] PDPA Section 15 pertains to deemed consent.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[4].
1.a) Does this privacy statement describe how personal information is collected?	If **YES**, the Accountability Agent must verify that: • The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. • The Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	**Policies and practices** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b).

[4] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules. For example, when the personal data collected/used/disclosed is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, or when personal data is publicly available.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		<u>Notification of purpose</u> 20. (1) For the purposes of sections 14(1)(a)[5] and 18(b), an organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15[6]; or

[5] PDPA Section 14(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;
[6] PDPA Section 15 pertains to deemed consent.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[7]. **<u>Advisory Guidelines on Key Concepts in the PDPA (Notification Obligation)</u>** 14.10 Relevant factors affecting an organisation's determination of the appropriate manner and form of notification to an individual of its purposes may include the following: a) the circumstances and manner in which it will be collecting the personal data; b) the amount of personal data to be collected; c) the frequency at which the personal data will be collected; and d) the channel through which the notification is provided (e.g. face-to-face or through a telephone conversation). 14.15 An organisation should state its purposes at an appropriate level of detail for the individual to determine the reasons and manner in which the organisation will be collecting, using or disclosing his personal data.
1.b) Does this privacy statement describe the	Where the Applicant answers **YES**, the Accountability Agent must verify that the applicant	**<u>Policies and practices</u>** 12. An organisation shall –

[7] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules. For example, when the personal data collected/used/disclosed is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, or when personal data is publicly available.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
purpose(s) for which personal information is collected?	provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[8] and 18(b), an organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the

[8] PDPA Section 14(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15[9]; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[10].
1.c) Does this privacy statement inform individuals whether their personal information is made available to third	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and	**Policies and practices** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

[9] PDPA Section 15 pertains to deemed consent.

[10] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules. For example, when the personal data collected/used/disclosed is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, or when personal data is publicly available.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
parties and for what purpose?	the purpose for which the personal information will or may be made available. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[11] and 18(b), an organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data.

[11] PDPA Section 14(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15[12]; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[13]. **Advisory Guidelines on Key Concepts in the PDPA (Consent Obligation)** 12.34 Organisations obtaining personal data from third party sources should exercise the appropriate due diligence to check and ensure that the third party source can validly give consent for the collection, use and disclosure of personal data on behalf of the individual (under section 14(4)) or that the source had

[12] PDPA Section 15 pertains to deemed consent.

[13] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules. For example, when the personal data collected/used/disclosed is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, or when personal data is publicly available.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		obtained consent for disclosure of the personal data (under section 15(2)). **<u>Advisory Guidelines on Key Concepts in the PDPA (Notification Obligation)</u>** 14.1 As noted in the previous sections on the Consent Obligation and the Purpose Limitation Obligation, organisations must inform individuals of the purposes for which their personal data will be collected, used and disclosed in order to obtain their consent. The organisation's collection, use and disclosure is limited to the purposes for which notification has been made to the individuals concerned. 14.16 In considering how specific to be when stating its purposes, organisations may have regard to the following: a) whether the purpose is stated clearly and concisely; b) whether the purpose is required for the provision or products or services (as distinct from optional purposes); c) if the personal data will be disclosed to other organisations, how the organisations should be made known to the individuals; d) whether stating the purpose to a greater degree of specificity would be a help or hindrance to the individual understanding the purpose(s) for which his personal data would be collected, used or disclosed; and

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		e) what degree of specificity would be appropriate in light of the organisation's business processes.
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a functional e-mail address. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	**<u>Compliance with Act</u>** 11. (3) An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act. (4) An individual designated under subsection (3) may delegate to another individual the responsibility conferred by that designation. (5) An organisation shall make available to the public the business contact information of at least one of the individuals designated under subsection (3) or delegated under subsection (4). **<u>Notification of purpose</u>** 20. (1) For the purposes of sections 14(1)(a)[14] and 18(b), an organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under

[14] PDPA Section 14(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. **Advisory Guidelines on Key Concepts in the PDPA (Openness Obligation)** 20.6 - As good practice, the business contact information of the relevant person should be readily accessible from Singapore, operational during Singapore business hours and in the case of telephone numbers, be Singapore telephone numbers. This is especially important if the relevant person is not physically based in Singapore. This would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices.
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that	**Policies and practices** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **<u>Notification of purpose</u>** 20. (1) For the purposes of sections 14(1)(a)[15] and 18(b), an organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act.

[15] PDPA Section 14(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15[16]; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[17]. **Advisory Guidelines on Key Concepts in the PDPA (Consent Obligation)** 12.34 Organisations obtaining personal data from third party sources should exercise the appropriate due diligence to check and ensure that the third party source can validly give consent for the collection, use and disclosure of personal data on behalf of the individual (under section 14(4)) or that the source had obtained consent for disclosure of the personal data (under section 15(2)). **Advisory Guidelines on Key Concepts in the PDPA (Notification Obligation)** 14.1 As noted in the previous sections on the Consent Obligation and the Purpose Limitation Obligation, organisations must inform individuals of the purposes for

[16] PDPA Section 15 pertains to deemed consent.

[17] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules. For example, when the personal data collected/used/disclosed is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, or when personal data is publicly available.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		which their personal data will be collected, used and disclosed in order to obtain their consent. The organisation's collection, use and disclosure is limited to the purposes for which notification has been made to the individuals concerned. 14.16 In considering how specific to be when stating its purposes, organisations may have regard to the following: a) whether the purpose is stated clearly and concisely; b) whether the purpose is required for the provision or products or services (as distinct from optional purposes); c) if the personal data will be disclosed to other organisations, how the organisations should be made known to the individuals; d) whether stating the purpose to a greater degree of specificity would be a help or hindrance to the individual understanding the purpose(s) for which his personal data would be collected, used or disclosed; and e) what degree of specificity would be appropriate in light of the organisation's business processes.
1.f) Does this privacy statement provide information regarding whether and how an individual can access	Where the Applicant answers **YES**, the Accountability Agent must verify that the Privacy Statement includes:	**Policies and practices** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
and correct their personal information?	• The process through which the individual may access his or her personal information (including electronic or traditional non- electronic means). • The process that an individual must follow in order to correct his or her personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Access to personal data** 21. (1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with – (a) personal data about the individual that is in the possession or under the control of the organisation; and (b) information about the ways in which the personal data referred to in paragraph (a) has been or may have been used or disclosed by the organisation within the year before the date of the request. (2) An organisation is not required to provide an individual with the individual's personal data or other information under subsection (1) in respect of the matters specified in the Fifth Schedule[18].

[18] PDPA Fifth Schedule – Exceptions from access requirement

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(3) An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to – (a) threaten the safety or physical or mental health of an individual other than the individual who made the request; (b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; (c) reveal personal data about another individual; (d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity or (e) be contrary to the national interest. (4) An organisation shall not inform any individual under subsection (1) that it has disclosed personal data to a prescribed law enforcement agency if the disclosure was made without the consent of the individual pursuant to paragraph 1(f) or (n) of the Fourth Schedule or under any other written law. (5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation shall provide the individual with access to the

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		personal data and other information without the personal data and other information excluded under subsections (2), (3) and (4). **<u>Correction of personal data</u>** 22. (1) An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation. (2) Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall – (a) correct the personal data as soon as practicable; and (b) subject to subsection (3), send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. (3) An organisation (not being a credit bureau) may, if the individual consents, send the corrected personal data only to specific organisations to which the personal data was disclosed by the organisation within a year before the date the correction was made. (4) When an organisation is notified under subsection (2)(b) or (2) of a correction of personal data, the organisation shall correct the personal data in its possession or under its control

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		unless the organisation is satisfied on reasonable grounds that the correction should not be made. (5) If no correction is made under subsection (2)(a) or (4), the organisation shall annotate the personal data in its possession or under its control with the correction that was requested but not made. (6) Nothing in this section shall require an organisation to correct or otherwise alter an opinion, including a professional or an expert opinion. (7) An organisation is not required to comply with this section in respect of the matters specified in the Sixth Schedule[19]. **PERSONAL DATA PROTECTION REGULATIONS 2014** Part II (Requests for access to and correction of personal data) of the Regulations elaborates on how organisations can respond to requests for access to and correction of personal data, including how to make the request, timeframe for response, and applicable fees.

[19] PDPA Sixth Schedule – Exceptions from correction requirement.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		How to make request 3.(1) A request to an organisation must be made in writing and shall include sufficient detail to enable the organisation, with a reasonable effort, to identify – (a) the applicant making the request (b) in relation to a request under section 21(1) of the Act, the personal data and use and disclosure information requested by the applicant; and (c) in relation to a request under section 22 of the Act, the correction requested by the applicant. (2) A request must be sent to the organisation – (a) in accordance with section 48A of the Interpretation Act (Cap.1); (b) by sending it to the organisation's data protection officer in accordance with the business contact information provided under section 11(5) of the Act; or (c) in such other manner as is acceptable to the organisation.
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected **and that the notice is reasonably available to individuals.** Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that	**Provision of consent** 14. (1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
that such information is being collected?	the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	**Limitation of purpose and extent** 18. An organisation may collect, use or disclose personal data about an individual only for purposes – (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable. **Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[20] and 18(b), an organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with

[20] PDPA Section 14(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15[21]; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[22]. (4) Notwithstanding subsection (3), an organisation, on or before collecting, using or disclosing the personal data about an individual for the purpose of managing or terminating an employment relationship between the organisation and that individual, shall inform the individual of – (a) that purpose; and (b) on request by the individual, the business contact information of a person who is able to answer the individual's questions about that collection, use or disclosure on behalf of the organisation.

[21] PDPA Section 15 pertains to deemed consent.

[22] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules. For example, when the personal data collected/used/disclosed is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, or when personal data is publicly available.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	**Provision of consent** 14. (1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act. **Limitation of purpose and extent** 18. An organisation may collect, use or disclose personal data about an individual only for purposes – (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable. **Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[23] and 18(b), an organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under

[23] PDPA Section 14(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15[24]; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[25].
4. Subject to the qualifications listed below, at the time of	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal	**Provision of consent**

[24] PDPA Section 15 pertains to deemed consent.

[25] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules. For example, when the personal data collected/used/disclosed is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, or when personal data is publicly available.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
collection of personal information, do you notify individuals that their personal information may be shared with third parties?	information will be or may be shared with third parties and for what purposes. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.	14. (1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act. **<u>Limitation of purpose and extent</u>** 18. An organisation may collect, use or disclose personal data about an individual only for purposes – (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable. **<u>Notification of purpose</u>** 20. (1) For the purposes of sections 14(1)(a)[26] and 18(b), an organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under

[26] PDPA Section 14(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15[27]; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[28]. **Advisory Guidelines on Key Concepts in the PDPA (Consent Obligation)**

[27] PDPA Section 15 pertains to deemed consent.

[28] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules. For example, when the personal data collected/used/disclosed is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, or when personal data is publicly available.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		12.34 Organisations obtaining personal data from third party sources should exercise the appropriate due diligence to check and ensure that the third party source can validly give consent for the collection, use and disclosure of personal data on behalf of the individual (under section 14(4)) or that the source had obtained consent for disclosure of the personal data (under section 15(2)). **Advisory Guidelines on Key Concepts in the PDPA (Notification Obligation)** 14.1 As noted in the previous sections on the Consent Obligation and the Purpose Limitation Obligation, organisations must inform individuals of the purposes for which their personal data will be collected, used and disclosed in order to obtain their consent. The organisation's collection, use and disclosure is limited to the purposes for which notification has been made to the individuals concerned. 14.16 In considering how specific to be when stating its purposes, organisations may have regard to the following: a) whether the purpose is stated clearly and concisely; b) whether the purpose is required for the provision or products or services (as distinct from optional purposes); c) if the personal data will be disclosed to other organisations, how the organisations should be made known to the individuals;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		d) whether stating the purpose to a greater degree of specificity would be a help or hindrance to the individual understanding the purpose(s) for which his personal data would be collected, used or disclosed; and e) what degree of specificity would be appropriate in light of the organisation's business processes.

COLLECTION LIMITATION

Assessment Purpose - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair.*

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
5. How do you obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf? 5.c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES** to any of these sub- parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	**Consent required** 13. An organisation shall not, on or before the appointed day, collect, use or disclose personal data about an individual unless – (a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law. **Provision of consent** 14. (1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act. (2) An organisation shall not –

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or (b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices. (3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act. (4) In this Act, references to consent given, or deemed to have been given by an individual shall include consent given, or deemed to have been given, by any person validly acting on behalf of that individual for the collection, use or disclosure of such personal data. **Limitation of purpose and extent** 18. An organisation may collect, use or disclose personal data about an individual only for purposes – (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		<u>Collection, use and disclosure without consent</u> 17. (1) An organisation may collect personal data about an individual, without consent or from a source other than the individual, only in the circumstances and subject to any condition in the Second Schedule. **<u>Advisory Guidelines on Key Concepts in the PDPA (Consent Obligation)</u>** 12.34 Organisations obtaining personal data from third party sources should exercise the appropriate due diligence to check and ensure that the third party source can validly give consent for the collection, use and disclosure of personal data on behalf of the individual (under section 14(4)) or that the source had obtained consent for disclosure of the personal data (under section 15(2)). In the event the third party source could not validly give consent or had not obtained consent for disclosure to the collecting organisation, but concealed this from the collecting organisation, the actions taken by the collecting organisation to verify such matters before collecting the personal data from the third party source would be considered a possible mitigating factor by the Commission should there be a breach of the PDPA relating to such collection or the collecting organisation's use or subsequent disclosure of the personal data.
6. Do you limit your personal information collection (whether	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other	**<u>Limitation of purpose and extent</u>** 18. An organisation may collect, use or disclose personal data about an individual only for purposes –

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	compatible or related purposes, the Accountability Agent must require the Applicant to identify: □ Each type of data collected; □ The corresponding stated purpose of collection for each; and □ All uses that apply to each type of data; □ An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection. Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	(a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable. **Advisory Guidelines on Key Concepts in the PDPA (Purpose Limitation Obligation)** 13.3 The main objective of the Purpose Limitation Obligation is to ensure that organisations collect, use and disclose personal data that is relevant for the purposes, and only for purposes that are reasonable. Consistent with the Notification Obligation, the Purpose Limitation Obligation also limits the purposes for which personal data may be collected, used or disclosed to those which have been informed to the individuals concerned pursuant to the Notification Obligation (where applicable). **Advisory Guidelines on Key Concepts in the PDPA (Notification Obligation)** 14.1 As noted in the previous sections on the Consent Obligation and the Purpose Limitation Obligation, organisations must inform individuals of the purposes for which their personal data will be collected, used and disclosed in order to obtain their consent. The organisation's collection, use and disclosure is limited to the purposes for which notification has been made to the individuals concerned. 14.5 It is important for an organisation to identify the purposes for which it is collecting, using or disclosing personal data by

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		establishing the appropriate policies and procedures. These would enable the organisation to identify what personal data it needs to collect, use and disclose for its business purposes and to ensure that the personal data collected in consistent with the purposes identified. It would also minimise the risk of collecting, using or disclosing personal data in contravention of the Data Protection Provisions.
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	**Provision of consent** 14.(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act. (2) An organisation shall not – (a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or (b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act. (4) In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about an individual shall include consent given, or deemed to have been given, by any personal validly acting on behalf of that individual for the collection, use or disclosure of such personal data. **Limitation of purpose and extent** 18. An organisation may collect, use or disclose personal data about an individual only for purposes – (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable.

USES OF PERSONAL INFORMATION

Assessment Purpose - *Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant.*

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	**Consent required** 13. An organisation shall not, on or before the appointed day, collect, use or disclose personal data about an individual unless – (a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law. **Provision of consent** 14.(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
description in the space below.		(2) An organisation shall not – (a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or (b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices. (3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act. (4) In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about an individual shall include consent given, or deemed to have been given, by any personal validly acting on behalf of that individual for the collection, use or disclosure of such personal data. **<u>Limitation of purpose and extent</u>** 18. An organisation may collect, use or disclose personal data about an individual only for purposes – (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		Notification of purpose 20. (1) For the purposes of sections 14(1)(a)[29] and 18(b), an organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15[30]; or

[29] PDPA Section 14(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;
[30] PDPA Section 15 pertains to deemed consent.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[31] **<u>Collection, use and disclosure without consent</u>** 17.(2) An organisation may use personal data about an individual, without the consent of the individual, only in the circumstances and subject to any condition in the Third Schedule.
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual?	Where the Applicant answers **NO** to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as: • Online at point of collection	**<u>Consent required</u>** 13. An organisation shall not, on or before the appointed day, collect, use or disclose personal data about an individual unless – (a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law. **<u>Collection, use and disclosure without consent</u>** 17.(2) An organisation may use personal data about an individual, without the consent of the individual, only in the

[31] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules. For example, when the personal data collected/used/disclosed is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, or when personal data is publicly available.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
9.b) Compelled by applicable laws?	• Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	circumstances and subject to any condition in the Third Schedule.
10. Do you disclose personal information you collect (whether	Where the Applicant answers **YES** in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal	**Consent required**

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.	information controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law. Also, the Accountability Agent must require the Applicant to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	13. An organisation shall not, on or before the appointed day, collect, use or disclose personal data about an individual unless – (a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law. **Provision of consent** 14.(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act. (2) An organisation shall not – (a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or (b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act. (4) In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about an individual shall include consent given, or deemed to have been given, by any personal validly acting on behalf of that individual for the collection, use or disclosure of such personal data. **Limitation of purpose and extent** 18. An organisation may collect, use or disclose personal data about an individual only for purposes – (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable. **Notification of purpose** 20.(1) For the purposes of sections 14(1)(a) and 18(b), and organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data; as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15; or (b) the organisation collects, uses or discloses the personal data without consent of the individual in accordance with section 17. **Transfer of personal data outside Singapore** 26.(1) An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		PERSONAL DATA PROTECTION REGULATIONS 2014 Part III (Transfer of personal data outside Singapore) of the Regulations provides for the requirements for transfer and legally enforceable obligations. Requirements for transfer 9.(1) For the purposes of section of 26 of the Act, a transferring organisation must, before transferring an individual's personal data to a country or territory outside Singapore – (a) take appropriate steps to ensure that the transferring organisation will comply with Parts III to VI of the Act, in respect of the transferred personal data while it remains in the possession or under the control of the transferring organisation; and (b) take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations (in accordance with regulation 10) to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act. (2) A transferring organisation is taken to have satisfied the requirements of paragraph 1(a) in respect of the transferred personal data while it remains in possession or under the control of the transferring organisation if the personal data is – (a) data in transit; or (b) publicly available in Singapore

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(3) A transferring organisation is taken to have satisfied the requirements of paragraph (1)(b) in respect of an individual's personal data which it transfers to a recipient in a country or territory outside Singapore if – (a) subject to paragraph (4), the individual consents to the transfer of the personal data to that recipient in that country or territory; (b) the transfer of the personal data to the recipient is necessary for the performance of a contract between the individual and the transferring organisation, or to do anything at the individual's request with a view to the individual entering into a contract with the transferring organisation; (c) the transfer of the personal data to the recipient is necessary for the conclusion of performance of a contract between the transferring organisation and a third party which is entered into at the individual's request; (d) the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organisation and a third party if a reasonable person would consider the contract to be in the individual's interest; (e) the transfer of the personal data to the recipient is necessary for the personal data to be used under paragraph 1(a), (b) or (d) of the Third Schedule of the Act or disclosed under paragraph 1(a), (b), (c), (e) or (o) of the Fourth Schedule to the Act, and the transferring organisation has taken reasonable steps to ensure that the personal data so transferred will not be used or disclosed by the recipient for any other purpose;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(f) the personal data is data in transit; or (g) the personal data is publicly available in Singapore. (4) An individual is not taken to have consented to the transfer of the individual's personal data to a country or territory outside Singapore if – (a) the individual was not, before giving his consent, given a reasonable summary in writing of the extent to which the personal data transferred to that country or territory will be protected to a standard comparable to the protection under the Act; (b) the transferring organisation required the individual to consent to the transfer as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual; or (c) the transferring organisation obtained or attempted to obtain the individual's consent for the transfer by providing false or misleading information about the transfer, or by using other deceptive or misleading practices. (5) Nothing in this Part prevents an individual from withdrawing any consent given for the transfer of the personal to a country or territory outside Singapore. **<u>Collection, use and disclosure without consent</u>** 17(3) An organisation may disclose personal data about an individual, without the consent of the individual, only in the

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		circumstances and subject to any condition in the Fourth Schedule.
11. Do you transfer personal information to personal information processors? If YES, describe.		*Please also refer to responses for question 10.* **<u>Application of the Act</u>** 4.(3) An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself. **<u>Withdrawal of consent</u>** 16.(4) Subject to section 25[32], if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation shall cease (and cause its data intermediaries[33] to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or other written law.
12. If you answered YES to question 10 and/or question 11, is		*Please also refer to responses for questions 10 and 11.*

[32] PDPA Section 25 pertains to retention of personal data

[33] Data intermediary means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.		
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances? 13.a) Based on express consent of the individual?	Where applicant answers **NO** to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers **YES** to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: □ Online at point of collection □ Via e-mail □ Via preference/profile page □ Via telephone □ Via postal mail, or □ Other (in case, specify)	*Please refer to responses for questions 10 and 11.*

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	Where the Applicant answers **YES** to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers **YES** to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
13.b) Necessary to provide a service or product requested by the individual?		*Please refer to responses for questions 10 and 11.*
13.c) Compelled by applicable laws?		*Please refer to responses for questions 10 and 11.*

CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice.*

These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification and the	**Consent required** 13. An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless – (a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law. **Provision of consent** 14.(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act. (2) An organisation shall not –

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	(a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about an individual beyond what is reasonable to provide the product or service to that individual; or (b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices. (3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act. (4) In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about the individual shall include consent given, or deemed to have been given, by any person validly acting on behalf of that individual for the collection, use or disclosure of such personal data. **Withdrawal of consent** 16.(1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(2) On receipt of the notice referred to in subsection (1), the organisation concerned shall inform the individual of likely consequences of withdrawing his consent. (3) An organisation shall not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section shall not affect any legal consequences arising from such withdrawal. (4) Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation shall cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or other written law.
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail	**<u>Consent required</u>** 13. An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless – (a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
YES describe such mechanisms below.	• Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: □ being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and □ Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and	**Provision of consent** 14.(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act. (2) An organisation shall not – (a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about an individual beyond what is reasonable to provide the product or service to that individual; or (b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices. (3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act. (4) In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about the individual shall include consent given, or deemed to have been given, by any person validly

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	acting on behalf of that individual for the collection, use or disclosure of such personal data. **Withdrawal of consent** 16.(1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose. (2) On receipt of the notice referred to in subsection (1), the organisation concerned shall inform the individual of likely consequences of withdrawing his consent. (3) An organisation shall not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section shall not affect any legal consequences arising from such withdrawal. (4) Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation shall cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or other written law.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: □ disclosing the personal information to third parties, other than Service Providers, for a purpose	**Consent required** 13. An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless – (a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law. **Provision of consent** 14.(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act. (2) An organisation shall not – (a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about an individual beyond what is reasonable to provide the product or service to that individual; or (b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices. (3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act. (4) In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about the individual shall include consent given, or deemed to have been given, by any person validly acting on behalf of that individual for the collection, use or disclosure of such personal data. **Withdrawal of consent** 16.(1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose. (2) On receipt of the notice referred to in subsection (1), the organisation concerned shall inform the individual of likely consequences of withdrawing his consent. (3) An organisation shall not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section shall not affect any legal consequences arising from such withdrawal.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(4) Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation shall cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or other written law.
17. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	**Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[34] and 18(b), an organisation shall inform the individual of – (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the

[34] PDPA Section 14(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by the organisation for a purpose unless – (a) the individual has been provided with the information required under section 20;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers **NO**, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) shall not apply if – (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15[35]; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[36].
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and	

[35] PDPA Section 15 pertains to deemed consent.

[36] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules. For example, when the personal data collected/used/disclosed is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, or when personal data is publicly available.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
personal information, are these choices easily accessible and affordable? Where YES, describe.	affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	**Policies and practices** 12. An organisation shall — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Consent required** 13. An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless – (a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law. **Provision of consent** 14.(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless – (a) the individual has been provided with the information required under section 20; and (b) the individual provided his consent for that purpose in accordance with this Act. (2) An organisation shall not – (a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about an individual beyond what is reasonable to provide the product or service to that individual; or (b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices. (3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act. (4) In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about the individual shall include consent

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		given, or deemed to have been given, by any person validly acting on behalf of that individual for the collection, use or disclosure of such personal data. **<u>Withdrawal of consent</u>** 16.(1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose. (2) On receipt of the notice referred to in subsection (1), the organisation concerned shall inform the individual of likely consequences of withdrawing his consent. (3) An organisation shall not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section shall not affect any legal consequences arising from such withdrawal. (4) Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation shall cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or other written law.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		<u>Advisory Guidelines on Key Concepts in the PDPA (Notification Obligation)</u> 12.42 The Commission considers that it would be difficult to take a one-size-fits-all approach and prescribe a specific time frame for reasonable notice to be given. However, as a general rule of thumb, the Commission would consider a withdrawal notice of at least ten (10) business days from the day the organisation receives the withdrawal notice, to be reasonable notice. Should an organisation require more time to give effect to a withdrawal notice, it is good practice for the organisation to inform the individual of the time frame by which the withdrawal of consent will take effect.

INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - *The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.*

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	**Accuracy of personal data** 23. An organisation shall make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data — (a) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or (b) is likely to be disclosed by the organisation to another organisation.
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not	**Policies and practices** 12. An organisation shall — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	(b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Correction of personal data** 22.(1) An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation. (2) Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall — (a) correct the personal data as soon as practicable; and (b) subject to subsection (3), send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. (3) An organisation (not being a credit bureau) may, if the individual consents, send the corrected personal data only to specific organisations to which the personal data was disclosed

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		by the organisation within a year before the date the correction was made. (4) When an organisation is notified under subsection (2)(b) or (3) of a correction of personal data, the organisation shall correct the personal data in its possession or under its control unless the organisation is satisfied on reasonable grounds that the correction should not be made. (5) If no correction is made under subsection (2)(a) or (4), the organisation shall annotate the personal data in its possession or under its control with the correction that was requested but not made. (6) Nothing in this section shall require an organisation to correct or otherwise alter an opinion, including a professional or an expert opinion. (7) An organisation is not required to comply with this section in respect of the matters specified in the Sixth Schedule[37].

[37] PDPA Sixth Schedule – Exceptions from correction requirement

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	**Application of the Act** 4.(2) Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data) shall not impose any obligation on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. (3) An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself. **Correction of personal data** 22.(1) An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation. (2) Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall — (a) correct the personal data as soon as practicable; and (b) subject to subsection (3), send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(3) An organisation (not being a credit bureau) may, if the individual consents, send the corrected personal data only to specific organisations to which the personal data was disclosed by the organisation within a year before the date the correction was made. (4) When an organisation is notified under subsection (2)(b) or (3) of a correction of personal data, the organisation shall correct the personal data in its possession or under its control unless the organisation is satisfied on reasonable grounds that the correction should not be made. (5) If no correction is made under subsection (2)(a) or (4), the organisation shall annotate the personal data in its possession or under its control with the correction that was requested but not made. (6) Nothing in this section shall require an organisation to correct or otherwise alter an opinion, including a professional or an expert opinion. (7) An organisation is not required to comply with this section in respect of the matters specified in the Sixth Schedule[38].

[38] PDPA Sixth Schedule – Exceptions from correction requirement

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		<u>Accuracy of personal data</u> 23. An organisation shall make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data — (a) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or (b) is likely to be disclosed by the organisation to another organisation.
24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties, to whom third parties to whom the personal information was disclosed? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	**<u>Correction of personal data</u>** 22. (1) An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation. (2) Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall — (a) correct the personal data as soon as practicable; and (b) subject to subsection (3), send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. (3) An organisation (not being a credit bureau) may, if the individual consents, send the corrected personal data only to specific organisations to which the personal data was disclosed

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		by the organisation within a year before the date the correction was made. (4) When an organisation is notified under subsection (2)(b) or (3) of a correction of personal data, the organisation shall correct the personal data in its possession or under its control unless the organisation is satisfied on reasonable grounds that the correction should not be made. (5) If no correction is made under subsection (2)(a) or (4), the organisation shall annotate the personal data in its possession or under its control with the correction that was requested but not made. (6) Nothing in this section shall require an organisation to correct or otherwise alter an opinion, including a professional or an expert opinion. (7) An organisation is not required to comply with this section in respect of the matters specified in the Sixth Schedule. **Accuracy of personal data** 23. An organisation shall make reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data – (a) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
		(b) is likely to be disclosed by the organisation to another organisation.
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	**Application of the Act** 4(3). An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself. **Compliance with Act** 11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control. **Accuracy of personal data** 23. An organisation shall make reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data – (a) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or (b) is likely to be disclosed by the organisation to another organisation.

SECURITY SAFEGUARDS

Assessment Purpose - *The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses*

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	**Compliance with Act** 11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control. **Policies and practices** 12. An organisation shall — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b).

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		Protection of personal data 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (eg password protections) • Encryption • Boundary protection (eg firewalls, intrusion detection) • Audit logging • Monitoring (eg external and internal audits, vulnerability scans) • Other (specify) The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party	**Protection of personal data** 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	
28. Describe how the safeguards you	Where the Applicant provides a description of the physical, technical and administrative safeguards	**Compliance with Act**

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control. **Policies and practices** 12. An organisation shall — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Protection of personal data** 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		<u>Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)</u> 17.2 - There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data. 17.3 - In practice, an organisation should: a) design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach; b) identify reliable and well-trained personnel responsible for ensuring information security; c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivities; and d) be prepared and able to respond to information security breaches promptly and effectively. 17.4 - In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. In doing so, the following factors may be considered:

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		a) the size of the organisation and the amount and type of personal data it holds; b) who within the organisation has access to the personal data; and c) whether the personal data is or will be held or used by a third party on behalf of the organisation.
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	**Policies and practices** 12. An organisation shall — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Protection of personal data** 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks,	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.	**Compliance with Act** 11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control. **Policies and practices** 12. An organisation shall — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Protection of personal data** 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
intrusions, or other security failures? 30.d) Physical security?		**<u>Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)</u>** 17.2 - There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data. 17.4 - In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. In doing so, the following factors may be considered: a) the size of the organisation and the amount and type of personal data it holds; b) who within the organisation has access to the personal data; and c) whether the personal data is or will be held or used by a third party on behalf of the organisation.
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information.	**<u>Policies and practices</u>** 12. An organisation shall — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	(b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Protection of personal data** 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	**Policies and practices** 12. An organisation shall — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b).

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		Protection of personal data 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.
33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	**Policies and practices** 12. An organisation shall — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Protection of personal data** 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		<u>Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)</u> 17.3 In practice, an organisation should: a) design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach; b) identify reliable and well-trained personnel responsible for ensuring information security; c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and d) be prepared and able to respond to information security breaches promptly and effectively. **<u>Guide to securing personal data in electronic medium</u>** 6.1 Holding regular assurance checks help organisations ensure that ICT security controls developed and configured for the protection of personal data are properly implemented and practised.
34. Do you use risk assessments or third-party certifications? Describe below.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	**<u>Protection of personal data</u>** 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. **<u>Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)</u>** 17.4 - In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		information security arrangements are adequate. In doing so, the following factors may be considered: a) the size of the organisation and the amount and type of personal data it holds; b) who within the organisation has access to the personal data; and c) whether the personal data is or will be held or used by a third party on behalf of the organisation.
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	**Application of the Act** 4(2) Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data) shall not impose any obligation on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. 4(3) An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself. **Policies and practices** 12. An organisation shall — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?		(c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Protection of personal data** 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. **Transfer of personal data outside Singapore** 26.(1) An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act. **Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)** 17.3 - In practice, an organisation should: a) design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		b) identify reliable and well-trained personnel responsible for ensuring information security; c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivities; and d) be prepared and able to respond to information security breaches promptly and effectively.

ACCESS AND CORRECTION

Assessment Purpose - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information.	**<u>Access to personal data</u>** 21.(1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with – (a) personal data about the individual that is in the possession or under the control of the organisation; and (b) information about the ways in which the personal data referred to in paragraph (a) has been or may have been used or disclosed by the organisation within a year before the date of the request. (2) An organisation is not required to provide an individual with the individual's personal data or other information under

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	subsection (1) in respect of the matters specified in the Fifth Schedule[39]. (3) An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to – (a) threaten the safety or physical or mental health of an individual other than the individual who made the request; (b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; (c) reveal personal data about another individual; (d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or (e) be contrary to the national interest. (4) An organisation shall not inform any individual under subsection (1) that it has disclosed personal data to a prescribed law enforcement agency if the disclosure was made without the

[39] PDPA Fifth Schedule – Exceptions from access requirement

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		consent of the individual pursuant to paragraph 1(f)[40] or (n)[41] of the Fourth Schedule or under any other written law. (5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation shall provide the individual with access to the personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4). **<u>Fifth Schedule – Exceptions from access requirement</u>** 1. An organisation is not required to provide information under section 21(1) in respect of – (j) any request – (iii) for information that does not exist or cannot be found.

[40] PDPA Fourth Schedule 1(f) – An organisation may disclose personal data about an individual without the consent of the individual when the disclosure is necessary for any investigation or proceedings. "Investigation" is defined under the PDPA to mean an investigation relating to – (a) a breach of an agreement; (b) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or (c) a circumstance or conduct that may result in a remedy or relief being available under any law. The term "proceedings" means any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of – (a) a breach or an agreement; (b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or (c) a wrong or a breach of a duty for which a remedy is claimed under any law.

[41] PDPA Fourth Schedule 1(n) – An organisation may disclose personal data about an individual without the consent of the individual when the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorization signed by the head of director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		PERSONAL DATA PROTECTION REGULATIONS 2014 **Part II: Requests for access to and correction of personal data** **Duty to respond to request under section 21(1) of Act** 4.(1) Subject to section 21(2), (3) and (4) of the Act and regulations 6 and 7(3), an organisation must respond to each request to it under section 21(1) of the Act as accurately and completely as necessary and reasonably possible. **Notification of timeframe for response** 5. Subject to the requirement to comply with section 21(1) of the Act as soon as reasonably possible or section 22(2) of the Act as soon as practicable, if the organisation is unable to comply with that requirement within 30 days after receiving a request made in accordance with regulation 3, the organisation must within that time inform the applicant in writing of the time by which it will respond to the request. **Refusal to confirm or deny existence, use or disclosure of personal data** 6. Subject to section 21(4) of the Act, an organisation, in response to a request to it under section 21(1) of the Act, may refuse to confirm or may deny – (a) the existence of personal data referred to in paragraph 1(h) of the Fifth Schedule to the Act; or

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(b) the use of personal data without consent under paragraph 1(e) of the Third Schedule to the Act or the disclosure of personal data without consent under paragraph 1(f) of the Fourth Schedule to the Act, for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed.
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information.	**<u>Access to personal data</u>** 21.(1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with – (a) personal data about the individual that is in the possession or under the control of the organisation; and (b) information about the ways in which the personal data referred to in paragraph (a) has been or may have been used or disclosed by the organisation within a year before the date of the request. (2) An organisation is not required to provide an individual with the individual's personal data or other information under subsection (1) in respect of the matters specified in the Fifth Schedule[42]. (3) An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other

[42] PDPA Fifth Schedule – Exceptions from access requirement

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of	Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	information, as the case may be, could reasonably be expected to – (a) threaten the safety or physical or mental health of an individual other than the individual who made the request; (b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; (c) reveal personal data about another individual; (d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or (e) be contrary to the national interest. (4) An organisation shall not inform any individual under subsection (1) that it has disclosed personal data to a prescribed law enforcement agency if the disclosure was made without the consent of the individual pursuant to paragraph 1(f)[43] or (n)[44] of the Fourth Schedule or under any other written law.

[43] PDPA Fourth Schedule 1(f) – An organisation may disclose personal data about an individual without the consent of the individual when the disclosure is necessary for any investigation or proceedings. "Investigation" is defined under the PDPA to mean an investigation relating to – (a) a breach of an agreement; (b) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or (c) a circumstance or conduct that may result in a remedy or relief being available under any law. The term "proceedings" means any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of – (a) a breach or an agreement; (b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or (c) a wrong or a breach of a duty for which a remedy is claimed under any law.

[44] PDPA Fourth Schedule 1(n) – An organisation may disclose personal data about an individual without the consent of the individual when the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorization signed by the head of director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
interaction with the individual (e.g. email, same language, etc)? 37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.		(5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation shall provide the individual with access to the personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4). **PERSONAL DATA PROTECTION REGULATIONS 2014** **Part II: Requests for access to and correction of personal data** **Duty to respond to request under section 21(1) of Act** 4.(1) Subject to section 21(2), (3) and (4) of the Act and regulations 6 and 7(3), an organisation must respond to each request to it under section 21(1) of the Act as accurately and completely as necessary and reasonably possible. (2) The organisation must provide an applicant access to the applicant's personal data requested under section 21(1) of the Act – (a) by providing the applicant a copy of the personal data and use and disclosure information in documentary form; (b) if sub-paragraph (a) is impracticable in any particular case, by allowing the applicant a reasonable opportunity to examine the personal data and use and disclosure information; or

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(c) in such other form requested by the applicant as is acceptable to the organisation. **Notification of timeframe for response** 5. Subject to the requirement to comply with section 21(1) of the Act as soon as reasonably possible or section 22(2) of the Act as soon as practicable, if the organisation is unable to comply with that requirement within 30 days after receiving a request made in accordance with regulation 3, the organisation must within that time inform the applicant in writing of the time by which it will respond to the request. **Refusal to confirm or deny existence, use or disclosure of personal data** 6. Subject to section 21(4) of the Act, an organisation, in response to a request to it under section 21(1) of the Act, may refuse to confirm or may deny – (a) the existence of personal data referred to in paragraph 1(h) of the Fifth Schedule to the Act; or (b) the use of personal data without consent under paragraph 1(e) of the Third Schedule to the Act or the disclosure of personal data without consent under paragraph 1(f) of the Fourth Schedule to the Act, for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		<u>Fees</u> 7.(1) Subject to section 28 of the Act, an organisation may charge an applicant who makes a request to it under section 21(1) of the Act a reasonable fee for services provided to the applicant to enable the organisation to respond to the applicant's request. (2) An organisation must not charge a fee to respond to the applicant's request under section 21(1) of the Act unless the organisation has — (a) provided the applicant with a written estimate of the fee; and (b) if the organisation wishes to charge a fee that is higher than the written estimate provided under sub-paragraph (a), notified the applicant in writing of the higher fee. (3) An organisation does not have to respond to an applicant's request under section 21(1) of the Act unless the applicant agrees to pay the following fee: (a) where the organisation has notified the applicant of a higher fee under paragraph (2)(b) - (i) if the Commission has reviewed the higher fee under section 28(1) of the Act, the fee allowed by the Commission under section 28(2) of the Act; or (ii) if sub-paragraph (i) does not apply, the higher fee notified under paragraph (2)(b); or

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(b) where sub-paragraph (a) does not apply and the organisation has provided the applicant with an estimated fee under paragraph (2)(a) — (i) if the Commission has reviewed the estimated fee under section 28(1) of the Act, the fee allowed by the Commission under section 28(2) of the Act; or (ii) if sub-paragraph (i) does not apply, the estimated fee provided under paragraph (2)(a). (4) For the avoidance of doubt, an organisation shall not charge the applicant any fee to comply with its obligations under section 22(2) of the Act.
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented	Where the Applicant answers **YES to questions 38a to 38e**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. necessary. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the	**<u>Correction of personal data</u>** 22.(1) An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation. (2) Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall – (a) correct the personal data as soon as practicable; and (b) subject to subsection (3), send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
in a clear and conspicuous manner? Provide a description in the space below or in an attachment if 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the	inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(3) An organisation (not being a credit bureau) may, if the individual consents, send the corrected personal data only to specific organisations to which the personal data was disclosed by the organisation within a year before the date the correction was made. (4) When an organisation is notified under subsection (2)(b) or (3) of a correction of personal data, the organisation shall correct the personal data in its possession or under its control unless the organisation is satisfied on reasonable grounds that the correction should not be made. (5) If no correction is made under subsection (2)(a) or (4), the organisation shall annotate the personal data in its possession or under its control with the correction that was requested but not made. (6) Nothing in this section shall require an organisation to correct or otherwise alter an opinion, including a professional or an expert opinion. (7) An organisation is not required to comply with this section in respect of the matters specified in the Sixth Schedule.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?		

ACCOUNTABILITY Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent.*

Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred.

However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) __ • Contracts __ • Compliance with applicable industry or sector laws and regulations __	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	**<u>Application of the Act</u>** 4.(6) Unless otherwise expressly provided in this Act – (a) Nothing in Parts III to VI shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening this Act; and (b) any provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law. **<u>Compliance with Act</u>** 11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
• Compliance with self- regulatory applicant code and/or rules __ • Other (describe) __		**<u>Policies and practices</u>** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b).
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable.	**<u>Compliance with Act</u>** 11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control. (3) An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	(4) An individual designated under subsection (3) may delegate to another individual the responsibility conferred by that designation. (5) An organisation shall make available to the public the business contact information of at least one of the individuals designated under subsection (3) or delegated under subsection (4). (6) The designation of an individual by an organisation under subsection (3) shall not relieve the organisation of any of its obligations under this Act.
41. Do you have procedures in place to receive, investigate and respond to privacy related complaints? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation	**<u>Policies and practices</u>** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b).

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
	of such procedures is required for compliance with this principle.	
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	**Policies and practices** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Advisory Guidelines on Key Concepts in the PDPA (Openness Obligation)** 20.6 - As good practice, the business contact information of the relevant person should be readily accessible from Singapore, operational during Singapore business hours and in the case of telephone numbers, be Singapore telephone numbers. This is especially important if the relevant person is not physically based in Singapore. This would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	**Policies and practices** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **Advisory Guidelines on Key Concepts in the PDPA (Openness Obligation)** 20.6 - As good practice, the business contact information of the relevant person should be readily accessible from Singapore, operational during Singapore business hours and in the case of telephone numbers, be Singapore telephone numbers. This is especially important if the relevant person is not physically based in Singapore. This would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices.
44. Do you have procedures in place for training	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its	**Policies and practices** 12. An organisation shall –

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	(a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b).
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	**<u>Application of the Act</u>** 4.(6) Unless otherwise expressly provided in this Act – (a) Nothing in Parts III to VI shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening this Act; and (b) any provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law. **<u>Compliance with Act</u>** 11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(2) An organisation is responsible for personal data in its possession or under its control. **<u>Policies and practices</u>** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **<u>Collection, use and disclosure without consent</u>** 17.(1) An organisation may collect personal data about an individual, without consent or from a source other than the individual, only in the circumstances and subject to any condition in the Second Schedule. (2) An organisation may use personal data about an individual, without the consent of the individual, only in the circumstances and subject to any condition in the Third Schedule.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(3) An organisation may disclose personal data about an individual, without the consent of the individual, only in the circumstances and subject to any condition in the Fourth Schedule
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? • Internal guidelines or policies __ • Contracts __ • Compliance with applicable industry or sector laws and regulations __	Where the Applicant answers **YES,** the Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	**Application of Act** 4.(2) Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data) shall not impose any obligation of a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. (3) An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself. **Compliance with Act** 11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
• Compliance with self- regulatory applicant code and/or rules __ • Other (describe) __		**<u>Policies and practices</u>** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b). **<u>Guide on data protection clauses for agreements relating to processing of personal data</u>** 6.21 - <u>Compliance with PDPA</u>: The Contractor shall comply with all its obligations under the PDPA at its own cost. [Clause 2.1 of the sample clauses requires the contractor to comply with all its obligations under the PDPA at its own costs] 6.22 - <u>Process, use and disclosure</u>: The Contractor shall only process, use and disclose Customer Personal Data: (a) strictly for the purposes of [fulfilling its obligations and providing the services required] under this Agreement; (b) with the Customer's prior written consent; or (c) when required by law or an order of court, but shall notify the Customer as soon as

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		practicable before complying with such law or order of court at its own costs. [Clause 2.2 of the sample clauses ensures that the contractor processes, uses or discloses customer personal data only under certain permitted circumstances. Where possible, clauses 2.2(a) should refer to the specific obligations of the contractor that require the processing, use or disclosure of personal data. Hence the phrase "fulfilling its obligations and providing the services required" may be amended or replaced as appropriate. Where a contractor has to process, use or disclose customer personal data in accordance with law or an order of court, clause 2.2(c) of the sample clauses requires the contractor to notify the customer as soon as practicable before complying with such law or order of court. This will give customers some time to obtain legal or professional advice before its customer personal data is processed, used or disclosed by the contractor in accordance with the law or order of court]
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your APEC- compliant privacy policies and	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	**Application of Act** 4.(2) Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data) shall not impose any obligation of a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. (3) An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
practices as stated in your Privacy Statement? __ • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? __ • Follow instructions provided by you relating to the manner in which your personal information must be handled? • Impose restrictions on subcontracting unless with your consent? __ • Have their CBPRs certified by an APEC accountability agent in their jurisdiction? __		its purposes by a data intermediary as if the personal data were processed by the organisation itself. **Compliance with Act** 11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control. **Policies and practices** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b).

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
• Notify the Applicant in the case of a breach of the personal information of the Applicant's customers? __ • Other (describe)		**<u>Guide on data protection clauses for agreements relating to processing of personal data</u>** 6.21 - <u>Compliance with PDPA</u>: The Contractor shall comply with all its obligations under the PDPA at its own cost. [Clause 2.1 of the sample clauses requires the contractor to comply with all its obligations under the PDPA at its own costs] 6.22 - <u>Process, use and disclosure</u>: The Contractor shall only process, use and disclose Customer Personal Data: (a) strictly for the purposes of [fulfilling its obligations and providing the services required] under this Agreement; (b) with the Customer's prior written consent; or (c) when required by law or an order of court, but shall notify the Customer as soon as practicable before complying with such law or order of court at its own costs. [Clause 2.2 of the sample clauses ensures that the contractor processes, uses or discloses customer personal data only under certain permitted circumstances. Where possible, clauses 2.2(a) should refer to the specific obligations of the contractor that require the processing, use or disclosure of personal data. Hence the phrase "fulfilling its obligations and providing the services required" may be amended or replaced as appropriate. Where a contractor has to process, use or disclose customer personal data in accordance with law or an order of court, clause 2.2(c) of the sample clauses requires the contractor to notify the customer as soon as practicable before complying

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		with such law or order of court. This will give customers some time to obtain legal or professional advice before its customer personal data is processed, used or disclosed by the contractor in accordance with the law or order of court]
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.	The Accountability Agent must verify the existence of such self-assessments.	**Application of Act** 4.(2) Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data) shall not impose any obligation of a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. (3) An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself. **Compliance with Act** 11.-(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control. **Policies and practices** 12. An organisation shall –

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (to be answered by the Economy) – SINGAPORE** **Personal Data Protection Act 2012 (No. 26 of 2012)**
		(a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b).
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other services providers to ensure compliance with your instructions and/or agreements/contracts? If yes, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	**Application of Act** 4.(2) Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data) shall not impose any obligation of a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. (3) An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		Compliance with Act 11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control. **Policies and practices** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and (ii) the complaint process referred to in paragraph (b).
50. Do you disclose personal information to other recipient persons or organizations in situations where due	If **YES**, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information,	**Application of Act** 4.(2) Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data) shall not impose any obligation of a data intermediary in respect of its processing of personal data on behalf of and for the

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	purposes of another organisation pursuant to a contract which is evidenced or made in writing. (3) An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself. **Compliance with Act** 11.(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control. **Policies and practices** 12. An organisation shall – (a) develop and implement policies and practices that are necessary for the organisation to meet its obligations of the organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and (d) make information available on request about – (i) the policies and practices referred to in paragraph (a); and

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (to be answered by the Economy) – SINGAPORE Personal Data Protection Act 2012 (No. 26 of 2012)
		(ii) the complaint process referred to in paragraph (b). **<u>Protection of personal data</u>** 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.