Annex B[1]

GLOBAL CBPR SYSTEM PROGRAM REQUIREMENTS: ENFORCEMENT MAP

*As outlined in Annex A of the Global CBPR Forum Terms of Reference, a jurisdiction interested in Membership ("**Applicant**") and intending to implement the Global CBPR and/or Global PRP System(s) should submit an explanation of how the Global CBPR and/or Global PRP System Program Requirements may be enforced in that jurisdiction.*

The purpose of this document is to assist Applicants in fulfilling the above-mentioned requirement. This document provides the Global CBPR System Program Requirements to guide an Applicant's explanation of how each Program Requirement may be enforced in its jurisdiction. The information provided by the Applicant will be considered in the Global CBPR Forum Membership Committee's recommendation on the application.

Column 1 lists the questions in the intake questionnaire to be answered by an Applicant Organisation when seeking Global CBPR certification. Column 2 lists the assessment criteria to be used by a Forum-recognized Accountability Agent when verifying the answers provided in Column 1. Column 3 is for use by the Applicant to explain the enforceability of an Applicant Organisation's answers in Column 1. Accountability Agents should be able to enforce the Global CBPR System Program Requirements through law or contract, and a jurisdiction'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 Global CBPR System Program Requirements. Additional documentation to assist in these explanations may be submitted as necessary.

Contents

[1] This document and the table that follows do not purport to provide a complete and comprehensive account of the Personal Data Protection Commission (PDPC) Singapore'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 Singapore or any other party and do not modify in any way the legal effect and interpretation of any laws.

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. The list of acceptable Qualifications to the Provision of Notice is below.*

Question	**Assessment Criteria**	**Enforceability - SINGAPORE** *Personal Data Protection Act 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 Organisation's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant Organisation'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 Global CBPR Framework; • Is easy to find and accessible; • Applies to all personal information, whether collected online or offline; and • States an effective date of privacy statement publication. Where Applicant Organisation answers **NO to question 1** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organisation that Notice as described herein is required for compliance with this Privacy Principle. Where the Applicant Organisation	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[2] and 18(b), an organisation must 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	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, must 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) does 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 15A or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[4].

[3] PDPA Section 15 pertains to deemed consent. Section 15A pertains to deemed consent by notification.

[4] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the These are elaborated under the First and Second 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
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 Organisation. • 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 Organisation that Notice as described herein is required for compliance with this Privacy Principle.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[5] and 18(b), an organisation must 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

[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;

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 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, must 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) does 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 15A; or (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

[6] PDPA Section 15 pertains to deemed consent. Section 15A pertains to deemed consent by notification.

[7] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the These are elaborated under the First and Second 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	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		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. 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 of 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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant Organisation answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must notify the Applicant Organisation that notice of the purposes for which personal information is collected is required and must be included in their privacy statement. Where the Applicant Organisation identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[8] and 18(b), an organisation must 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

[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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 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, must 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) does 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 15A; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[10]. **<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

[9] PDPA Section 15 pertains to deemed consent. Section 15A pertains to deemed consent by notification.
[10] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the These are elaborated under the First and Second 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	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		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. 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 of 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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation notifies individuals that their personal information will or may be made available to third parties, **identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available.** Where the Applicant Organisation answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must notify the Applicant Organisation that notice that personal information will be available to third parties is required and must be included in their privacy statement. Where the Applicant Organisation identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[11] and 18(b), an organisation must 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

[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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 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, must 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) does 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 15A; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[13]. **<u>Advisory Guidelines on Key Concepts in the PDPA (Consent Obligation)</u>** 12.33 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

[12] PDPA Section 15 pertains to deemed consent. Section 15A pertains to deemed consent by notification.

[13] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the First and Second 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		of the individual (under section 14(4)) or that the source had obtained consent for disclosure of the personal data (under section 15). **<u>Advisory Guidelines on Key Concepts in the PDPA (Notification Obligation)</u>** 14.1 As noted in the previous chapters 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 of 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 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 Organisation's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation provides name, address and a **functional** e-mail address. Where the Applicant Organisation answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organisation that such disclosure of information is required for compliance with this Privacy Principle. Where the Applicant Organisation identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	**Compliance with Act** 11. (3) An organisation must 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 must 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). **Notification of purpose** 20. (1) For the purposes of sections 14(1)(a)[14] and 18(b), an organisation must 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

[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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 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. **Advisory Guidelines on Key Concepts in the PDPA (Accountability Obligation)** 21.7 - The business contact information of the relevant person may be provided on BizFile+ for companies that are registered with ACRA, or provided in a readily accessible part of the organisation's official website such that it can be easily found. It 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 Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation'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.	**Policies and practices** 12. An organisation must – (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	Where the Applicant Organisation answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organisation, that such information is required for compliance with this Privacy Principle. Where the Applicant Organisation 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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **<u>Notification of purpose</u>** 20. (1) For the purposes of sections 14(1)(a)[15] and 18(b), an organisation must 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.

[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	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		(2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, must 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) does 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 15A; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[17]. **<u>Advisory Guidelines on Key Concepts in the PDPA (Consent Obligation)</u>** 12.33 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).

[16] PDPA Section 15 pertains to deemed consent. Section 15A pertains to deemed consent by notification.

[17] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the First and Second 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts in the PDPA (Notification Obligation)</u> 14.1 As noted in the previous chapters on the Consent Obligation and the PurposeLimitation 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 of 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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the privacy statement includes: • 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 Organisation answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organisation that providing information about access and correction, including the Applicant Organisation's typical response times for access and correction requests, is required for compliance with this Privacy Principle. Where the Applicant Organisation identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **Access to personal data** 21. (1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation must, 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 mentioned 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

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		information under subsection (1) in respect of the matters specified in the Fifth Schedule[18]. (3) Subject to subsection (3A), an organisation must 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. (3A) Subsection (3)(c) and (d) does not apply to any user activity data about, or any user provided data from, the individual who made the request despite such data containing personal data about another individual. (4) An organisation must not inform any individual under subsection (1)(b) that it has disclosed personal

[18] PDPA Fifth Schedule – Exceptions from access requirement.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		data to a prescribed law enforcement agency if the disclosure was made under this Act or under any other written law without the individual's consent. (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 must provide the individual with access to the 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 must – (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

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		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 (3) of a correction of personal data, the organisation must 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 must 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 requires 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].

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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		PERSONAL DATA PROTECTION REGULATIONS 2021 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. **How to make request** 3.(1) A request to an organisation must be made in writing and must 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(1) 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(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 that such information is being collected?	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation 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 Organisation answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organisation that the notice that personal information is being collected is required for compliance with this Privacy Principle. Where the Applicant Organisation 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)[20] and 18(b), an organisation must 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;

[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	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		(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, must 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) does 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 15A; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[22]. (4) Despite subsection (3), an organisation must comply with subsection (5) on or before collecting,

[21] PDPA Section 15 pertains to deemed consent. Section 15A pertains to deemed consent by notification.

[22] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the First and Second 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		using or disclosing personal data about an individual for the purpose of or in relation to the organisation — (a) entering into an employment relationship with the individual or appointing the individual to any office; or (b) managing or terminating the employment relationship with or appointment of the individual. (5) For the purposes of subsection (4), the organisation must inform the individual of the following: (a) the purpose for which the organisation is collecting, using or disclosing (as the case may be) the personal data about the individual; (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 (as the case may be) on behalf of the organisation.
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 Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation 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 Organisation's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant Organisation answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organisation of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant Organisation identifies an	**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 –

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	(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)[23] and 18(b), an organisation must 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, must 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.

[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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(3) Subsection (1) does 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 15A; 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 collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant Organisation answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organisation to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant Organisation identifies an applicable Qualification, the Accountability Agent must determine 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.

[24] PDPA Section 15 pertains to deemed consent. Section 15A pertains to deemed consent by notification.
[25] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the First and Second 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		Notification of purpose 20. (1) For the purposes of sections 14(1)(a)[26] and 18(b), an organisation must 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, must 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) does 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 15A; or

[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;
[27] PDPA Section 15 pertains to deemed consent. Section 15A pertains to deemed consent by notification.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(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)** 12.33 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). **Advisory Guidelines on Key Concepts in the PDPA (Notification Obligation)** 14.1 As noted in the previous chapters 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.

[28] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the First and Second 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	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		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 of 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.

Qualifications to the Provision of Notice

The following are situations in which the application at the time of collection of the Global CBPR Notice Principle may not be necessary or practical.

i. **Obviousness:** Personal information controllers do not need to provide notice of the collection, use or third-party sharing of personal information in those circumstances where consent by the individual can be inferred from the provision of the individual's information (e.g., if an individual gives his or her business card to another individual in the context of a business relationship, the individual would not expect that notice would be provided regarding the collection and normal use of that information).

ii. **Collection of Publicly-Available Information**: Personal information controllers do not need to provide notice regarding the collection and use of publicly available information.

iii. **Technological Impracticability**: Personal information controllers do not need to provide notice at or before the time of collection in those cases where electronic technology automatically collects information when a prospective customer initiates contact (e.g., through the use of cookies). However, the notice should be provided to the individuals as soon after as is practicable.

iv. **Disclosure to a government institution which has made a request for the information with lawful authority:** Personal information controllers do not need to provide notice of disclosure to law enforcement agencies for investigation purposes where the provision of such notice to the individual will likely prejudice the investigation.

v. **Disclosure to a third party pursuant to a lawful form of process:** Personal information controllers do not need to provide notice of disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.

vi. **Third-Party Receipt**: Where personal information is received from a third party, the recipient personal information controller does not need to provide notice to the individuals at or before the time of collection of the information.

vii. **For legitimate investigation purposes:** When providing notice would compromise the availability or accuracy of the information and the collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.

viii. **Action in the event of an emergency**: Personal information controllers do not need to provide notice in emergency situations that threaten the life, health or security of an individual.

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	**Assessment Criteria**	**Enforceability - SINGAPORE** *Personal Data Protection Act 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 Organisation indicates from whom they obtain personal information. Where the Applicant Organisation answers **YES to any of these sub-parts**, the Accountability Agent must verify the Applicant Organisation'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 Organisation that it has incorrectly completed the questionnaire.	**<u>Consent required</u>** 13. An organisation must not, on or after 2 July 2014, 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>Provision of consent</u>** 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 must not –

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 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 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. **<u>Deemed Consent</u>** 15.(1) An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose if — (a) the individual, without actually giving consent mentioned in section 14, voluntarily provides the personal data to the organisation for that purpose; and

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(b) it is reasonable that the individual would voluntarily provide the data. (2) If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation. **<u>Deemed consent by notification</u>** 15A.(1) This section applies to the collection, use or disclosure of personal data about an individual by an organisation on or after 1 February 2021. (2) Subject to subsection (3), an individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation if — (a) the organisation satisfies the requirements in subsection (4); and (b) the individual does not notify the organisation, before the expiry of the period mentioned in subsection (4)(b)(iii), that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organisation. [40/2020]

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(3) Subsection (2) does not apply to the collection, use or disclosure of personal data about the individual for any prescribed purpose. (4) For the purposes of subsection (2)(a), the organisation must, before collecting, using or disclosing any personal data about the individual — (a) conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual; (b) take reasonable steps to bring the following information to the attention of the individual: (i) the organisation's intention to collect, use or disclose the personal data; (ii) the purpose for which the personal data will be collected, used or disclosed; (iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the personal data; and (c) satisfy any other prescribed requirements. (5) The organisation must, in respect of the assessment mentioned in subsection (4)(a) — (a) identify any adverse effect that the proposed collection, use or disclosure of the personal data for the purpose concerned is likely to have on the individual;

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(b) identify and implement reasonable measures to — (i) eliminate the adverse effect; (ii) reduce the likelihood that the adverse effect will occur; or (iii) mitigate the adverse effect; and (c) comply with any other prescribed requirements. **<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>Collection, use and disclosure without consent</u>** 17. (1) An organisation may collect personal data about an individual, without the individual's consent or from a source other than the individual, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 1 of the Second Schedule.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts in the PDPA (Consent Obligation)</u> 12.18 Sections 15 and 15A of the PDPA provide for different forms of deemed consent, namely (a) deemed consent by conduct; (b) deemed consent by contractual necessity; and (c) deemed consent by notification. 12.33 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). 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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
6. Do you limit your personal information collection (whether 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?	Where the Applicant Organisation answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant Organisation to identify: • Each type of data collected; • The corresponding stated purpose of collection for each; • All uses that apply to each type of data; and • 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 Organisation limits the amount and type of personal information to that which is relevant to fulfill the stated purposes. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation 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.	**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. **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 are 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 chapters 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		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 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 is 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 Organisation answers **YES,** the Accountability Agent must require the Applicant Organisation 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 Organisation answers **NO**, the Accountability Agent must inform that Applicant Organisation that lawful and fair procedures are required for compliance with this Privacy Principle.	**<u>Provision of consent</u>** 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 must 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(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 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>Deemed Consent</u>** 15.(1) An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose if — (a) the individual, without actually giving consent mentioned in section 14, voluntarily provides the personal data to the organisation for that purpose; and (b) it is reasonable that the individual would voluntarily provide the data. (2) If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation. **<u>Deemed consent by notification</u>** 15A.(1) This section applies to the collection, use or disclosure of personal data about an individual by an organisation on or after 1 February 2021. (2) Subject to subsection (3), an individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation if — (a) the organisation satisfies the requirements in subsection (4); and (b) the individual does not notify the organisation, before the expiry of the period mentioned in subsection (4)(b)(iii), that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organisation. [40/2020] (3) Subsection (2) does not apply to the collection, use or disclosure of personal data about the individual for any prescribed purpose. (4) For the purposes of subsection (2)(a), the organisation must, before collecting, using or disclosing any personal data about the individual — (a) conduct an assessment to determine that the proposed collection, use or disclosure of the personal

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		data is not likely to have an adverse effect on the individual; (b) take reasonable steps to bring the following information to the attention of the individual: (i) the organisation's intention to collect, use or disclose the personal data; (ii) the purpose for which the personal data will be collected, used or disclosed; (iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the personal data; and (c) satisfy any other prescribed requirements. (5) The organisation must, in respect of the assessment mentioned in subsection (4)(a) — (a) identify any adverse effect that the proposed collection, use or disclosure of the personal data for the purpose concerned is likely to have on the individual; (b) identify and implement reasonable measures to — (i) eliminate the adverse effect; (ii) reduce the likelihood that the adverse effect will occur; or (iii) mitigate the adverse effect; and (c) comply with any other prescribed requirements.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Collection, use and disclosure without consent</u> 17.(1) An organisation may — (a) collect personal data about an individual, without the individual's consent or from a source other than the individual, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 1 of the Second Schedule; **<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.

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 Privacy 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 Organisation for the purpose of granting credit for the subsequent purpose of collecting debt owed to that Applicant Organisation.*

Question	**Assessment Criteria**	**Enforceability - SINGAPORE** *Personal Data Protection Act 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 description in the space below.	Where the Applicant Organisation 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 Organisation's privacy statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Organisation Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	**<u>Consent required</u>** 13. An organisation must not, on or 2 July 2014, 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>Provision of consent</u>** 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

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		the individual provided his consent for that purpose in accordance with this Act. (2) An organisation must 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 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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Deemed Consent</u> 15.(1) An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose if — (a) the individual, without actually giving consent mentioned in section 14, voluntarily provides the personal data to the organisation for that purpose; and (b) it is reasonable that the individual would voluntarily provide the data. (2) If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation. **<u>Deemed consent by notification</u>** 15A.(1) This section applies to the collection, use or disclosure of personal data about an individual by an organisation on or after 1 February 2021. (2) Subject to subsection (3), an individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation if — (a) the organisation satisfies the requirements in subsection (4); and

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		(b) the individual does not notify the organisation, before the expiry of the period mentioned in subsection (4)(b)(iii), that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organisation. [40/2020] (3) Subsection (2) does not apply to the collection, use or disclosure of personal data about the individual for any prescribed purpose. (4) For the purposes of subsection (2)(a), the organisation must, before collecting, using or disclosing any personal data about the individual — (a) conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual; (b) take reasonable steps to bring the following information to the attention of the individual: (i) the organisation's intention to collect, use or disclose the personal data; (ii) the purpose for which the personal data will be collected, used or disclosed; (iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the personal data; and (c) satisfy any other prescribed requirements. (5) The organisation must, in respect of the assessment mentioned in subsection (4)(a) —

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(a) identify any adverse effect that the proposed collection, use or disclosure of the personal data for the purpose concerned is likely to have on the individual; (b) identify and implement reasonable measures to — (i) eliminate the adverse effect; (ii) reduce the likelihood that the adverse effect will occur; or (iii) mitigate the adverse effect; and (c) comply with any other prescribed requirements. **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)[29] and 18(b), an organisation must inform the individual of –

[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;

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		(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, must 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) does 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 15A; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[31].

[30] PDPA Section 15 pertains to deemed consent. Section 15A pertains to deemed consent by notification.

[31] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the First and Second 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		Collection, use and disclosure without consent 17.(1) An organisation may — (b) use personal data about an individual without the individual's consent, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 2 of the Second 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? 9.b) Compelled by applicable laws?	Where the Applicant Organisation answers **NO** to question 8, the Applicant Organisation must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the Applicant Organisation selects 9a, the Accountability Agent must require the Applicant Organisation to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant Organisation's use of the personal information is based on express consent of the individual (9.a), such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant Organisation answers 9.a, the Accountability Agent must require the Applicant Organisation to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below.	**Consent required** 13. An organisation must not, on or before 2 July 2014, 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. **Collection, use and disclosure without consent** 17.(1) An organisation may — (b) use personal data about an individual without the individual's consent, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 2 of the Second Schedule. **Advisory Guidelines on Key Concepts in the PDPA (The Consent Obligation)** 12.55 Section 17 of the PDPA permits the collection, use and disclosure of personal data without consent (and, in the case of collection, from a source other than the individual) and enumerates the permitted

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	Where the Applicant Organisation selects 9.b, the Accountability Agent must require the Applicant Organisation to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant Organisation does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant Organisation 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 Privacy Principle.	purposes in the First and Second Schedules to the PDPA. These exceptions to the Consent Obligation do not affect rights or obligations arising under any other law. Hence, even if an exception applies under the PDPA, organisations are required to comply with their other legal obligations, for example, to protect confidential information or other contractual obligations.
10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.	Where the Applicant Organisation answers **YES** in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal 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 Organisation 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	**<u>Consent required</u>** 13. An organisation must not, on or before 2 July 2014, 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>Provision of consent</u>** 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	Accountability Agent must verify that the Applicant Organisation's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	(b) the individual provided his consent for that purpose in accordance with this Act. (2) An organisation must 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 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>Deemed Consent</u>** 15.(1) An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose if —

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(a) the individual, without actually giving consent mentioned in section 14, voluntarily provides the personal data to the organisation for that purpose; and (b) it is reasonable that the individual would voluntarily provide the data. (2) If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation. **<u>Deemed consent by notification</u>** 15A.(1) This section applies to the collection, use or disclosure of personal data about an individual by an organisation on or after 1 February 2021. (2) Subject to subsection (3), an individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation if — (a) the organisation satisfies the requirements in subsection (4); and (b) the individual does not notify the organisation, before the expiry of the period mentioned in subsection (4)(b)(iii), that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organisation.

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		[40/2020] (3) Subsection (2) does not apply to the collection, use or disclosure of personal data about the individual for any prescribed purpose. (4) For the purposes of subsection (2)(a), the organisation must, before collecting, using or disclosing any personal data about the individual — (a) conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual; (b) take reasonable steps to bring the following information to the attention of the individual: (i) the organisation's intention to collect, use or disclose the personal data; (ii) the purpose for which the personal data will be collected, used or disclosed; (iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the personal data; and (c) satisfy any other prescribed requirements. (5) The organisation must, in respect of the assessment mentioned in subsection (4)(a) — (a) identify any adverse effect that the proposed collection, use or disclosure of the personal data for

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		the purpose concerned is likely to have on the individual; (b) identify and implement reasonable measures to — (i) eliminate the adverse effect; (ii) reduce the likelihood that the adverse effect will occur; or (iii) mitigate the adverse effect; and (c) comply with any other prescribed requirements. **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 must 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

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		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, must 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) does 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 15A; or (b) the organisation collects, uses or discloses the personal data without consent of the individual in accordance with section 17. **<u>Transfer of personal data outside Singapore</u>** 26.(1) An organisation must 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		transferred that is comparable to the protection under this Act. **PERSONAL DATA PROTECTION REGULATIONS 2021** Part III (Transfer of personal data outside Singapore) of the Regulations provides for the requirements for transfer and legally enforceable obligations. **Requirements for transfer** 10.—(1) For the purposes of section 26 of the Act, a transferring organisation must, before transferring an individual's personal data to a country or territory outside Singapore on or after 1 February 2021, take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data is bound by legally enforceable obligations (in accordance with regulation 11) 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) 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 (3), the individual consents to the transfer of the individual's personal data to that recipient in that country or territory; (b) the individual is deemed to have consented to the disclosure by the transferring organisation of the

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		individual's personal data to that recipient under section 15(3), (4), (5), (6), (7) or (8) of the Act; (c) the transfer of the personal data to the recipient is necessary for the personal data to be used or disclosed under Part 1 or paragraph 2 of Part 2 of the First 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; (d) the personal data is data in transit; or (e) the personal data is publicly available in Singapore. (3) For the purposes of paragraph (2)(a), 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 or her consent, given a reasonable summary in writing of the extent to which the personal data to be 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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(4) This Part does not prevent an individual from withdrawing any consent given for the transfer of the personal data to a country or territory outside Singapore. **<u>Collection, use and disclosure without consent</u>** 17.—(1) An organisation may — (a) collect personal data about an individual, without the individual's consent or from a source other than the individual, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 1 of the Second Schedule; (b) use personal data about an individual without the individual's consent, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 2 of the Second Schedule; or (c) disclose personal data about an individual without the individual's consent, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 3 of the Second Schedule. (2) Unless otherwise provided under this Act, an organisation may — (a) collect personal data about an individual that the organisation receives by way of a disclosure to the organisation — (i) on or after 1 February 2021 in accordance with subsection (1)(c); or (ii) before 1 February 2021 in accordance with section 17(3) as in force before that date, for purposes consistent with the purpose of that

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		disclosure, or for any purpose permitted by subsection (1)(a); or (b) use or disclose personal data about an individual that — (i) is collected by the organisation on or after 1 February 2021 in accordance with subsection (1)(a); or (ii) was collected by the organisation before 1 February 2021 in accordance with section 17(1) as in force before that date, for purposes consistent with the purpose of that collection, or for any purpose permitted by subsection (1)(b) or (c), as the case may be.
11. Do you transfer personal information to personal information processors? If YES, describe.		*Please also refer to responses for question 10 on the Transfer Limitation Obligation.* **<u>Application of the Act</u>** 4.(3) An organisation has 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>Advisory Guidelines on Key Concepts in the PDPA (The Transfer Limitation Obligation)</u>** 19.7 As good practice, organisations are encouraged to rely on these circumstances only if they are unable to rely on legally enforceable obligations or specified certifications: a) the individual whose personal data is to be transferred gives his consent to the transfer of his

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		personal data, after he has been informed about how his personal data will be protected in the destination country; **<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 must 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 the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.		*Please also refer to responses for questions 10 and 11 on the Transfer Limitation Obligation..*
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take	Where Applicant Organisation answers **NO** to question 13, the Applicant Organisation must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes.	*Please refer to responses for questions 10 and 11 on the Transfer Limitation Obligation.* **<u>Advisory Guidelines on Key Concepts in the PDPA (The Transfer Limitation Obligation)</u>**

[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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
place under one of the following circumstances? 13.a) Based on express consent of the individual?	Where the Applicant Organisation answers **YES** to 13.a, the Accountability Agent must require the Applicant Organisation 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). Where the Applicant Organisation answers **YES** to 13.b, the Accountability Agent must require the Applicant Organisation 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 Organisation answers **YES** to 13.c, the Accountability Agent must require the Applicant Organisation to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant Organisation must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant Organisation is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement.	19.7 As good practice, organisations are encouraged to rely on these circumstances only if they are unable to rely on legally enforceable obligations or specified certifications: fa) the individual whose personal data is to be transferred gives his consent to the transfer of his personal data, after he has been informed about how his personal data will be protected in the destination country; b) the individual is deemed to have consented to the disclosure by the transferring organisation of the individual's personal data where the transfer is reasonably necessary for the conclusion or performance of a contract between the organisation and the individual, including the transfer to a third party organisation); c) the transfer is necessary for a use or disclosure that is in the vital interests of individuals or in the national interest, and the transferring organisation has taken reasonable steps to ensure that the personal data will not be used or disclosed by the recipient for any other purpose; d) the personal data is data in transit; or e) the personal data is publicly available in Singapore.
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.*

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	Where the Applicant Organisation answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant Organisation 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 Privacy Principle.	

CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Privacy 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 the Qualifications to the Provision of Choice Mechanisms listed below.*

Question	**Assessment Criteria**	**Enforceability - SINGAPORE** *Personal Data Protection Act 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 Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation 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 Organisation answers **NO**, the Applicant Organisation must identify the applicable Qualification and the Accountability Agent must verify whether the applicable Qualification is justified. Where the Applicant Organisation answers **NO** and does not identify an applicable Qualification the	**Consent required** 13. An organisation must not, on or after 2 July 2014, 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 must not –

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	Accountability Agent must inform the Applicant Organisation 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 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. **<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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(2) On receipt of the notice mentioned in subsection (1), the organisation concerned must inform the individual of the likely consequences of withdrawing his consent. (3) An organisation must not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section does 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 must 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 YES, describe such mechanisms below.	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation 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; • Via preference/profile page;	**<u>Consent required</u>** 13. An organisation must not, on or after 2 July 2014, 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	• 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 Organisation answers **NO**, the Applicant Organisation 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 Organisation answers **NO** and does not identify an acceptable Qualification, the Accountability Agent must inform the Applicant Organisation a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	**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 must 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 include consent given, or deemed to have been given, by any person validly acting on

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		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 mentioned in subsection (1), the organisation concerned must inform the individual of the likely consequences of withdrawing his consent. (3) An organisation must not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section does 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 must 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		of the individual is required or authorised under this Act or other written law. **<u>Advisory Guidelines on Key Concepts in the PDPA (The Consent Obligation)</u>** <u>Obtaining consent from an individual</u> 12.3 Section 14(1) of the PDPA states how an individual gives consent under the PDPA. An individual has not given consent unless the individual has been notified of the purposes for which his personal data will be collected, used or disclosed and the individual has provided his consent for those purposes. If an organisation fails to do so, any consent obtained from the individual would be invalid. 12.4 Consent can be obtained in several ways. Consent that is obtained in writing or recorded in a manner that is accessible is referred to in these Guidelines as 'express consent'. Such consent provides the clearest indication that the individual has consented to notified purposes of the collection, use or disclosure of his personal data. 12.5 In situations where it may be impractical for the organisation to obtain express consent in writing, it may choose to obtain verbal consent. As good practice, organisations can consider adopting the following practices in cases when consent is obtained verbally, to prove that verbal consent had been given, in the event of disputes:

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		a) Confirm the consent in writing with the individual (which may be in electronic form or other form of documentary evidence); or b) Where appropriate in the circumstances, make a written note (which may be in electronic form or other form of documentary evidence) of the fact that an individual had provided verbal consent.
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 Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation 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:	**Consent required** 13. An organisation must 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 must not –

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	• disclosing the personal information to third parties, other than service providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant Organisation'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 Organisation answers **NO**, the Applicant Organisation must identify the applicable Qualification and provide a description and the Accountability Agent must verify whether the applicable Qualification is justified. Where the Applicant Organisation answers **NO** and does not identify an acceptable Qualification, the Accountability Agent must inform the Applicant Organisation that a mechanism for individuals to exercise choice in relation to the disclosure 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 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. **<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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(2) On receipt of the notice mentioned in subsection (1), the organisation concerned must inform the individual of the likely consequences of withdrawing his consent. (3) An organisation must not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section does 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 must 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	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation's choice mechanism is displayed in a clear and conspicuous manner. Where the Applicant Organisation answers **NO**, or when the Accountability Agent finds that the Applicant Organisation's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant Organisation that all mechanisms that allow individuals to exercise choice in relation to	**<u>Notification of purpose</u>** 20. (1) For the purposes of sections 14(1)(a)[34] and 18(b), an organisation must 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

[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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
clear and conspicuous manner?	the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this Privacy Principle.	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, must 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) does 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 15A; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17[36].
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 Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation's choice mechanism is clearly worded and easily understandable. Where the Applicant Organisation answers **NO**, and/or when the Accountability Agent finds that the Applicant Organisation's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant Organisation 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 Privacy Principle.	
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 personal information, are these choices easily accessible	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation's choice mechanism is easily accessible and affordable. Where the Applicant Organisation answers **NO**, or when the Accountability Agent finds that the Applicant Organisation's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant Organisation that all mechanisms that allow individuals to exercise choice in relation to the collection,	

[35] PDPA Section 15 pertains to deemed consent. Section 15A pertains to deemed consent by notification.

[36] PDPA Section 17 relates to circumstances where an organisation may collect, use and disclose personal data without consent. These are elaborated under the First and Second 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
and affordable? Where YES, describe.	use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this Privacy 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 Organisation does have mechanisms in place, the Accountability Agent must require the Applicant Organisation 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 Organisation does not have mechanisms in place, the Applicant Organisation 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 Organisation answers **NO** and does not provide an acceptable Qualification, the Accountability Agent must inform the Applicant Organisation that a mechanism to ensure that choices, when offered, can be honored, must be provided.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **Consent required** 13. An organisation must 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 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. **<u>Provision of consent</u>** 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 must 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		collection, use or disclosure of personal data about the individual 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. **<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 mentioned in subsection (1), the organisation concerned must inform the individual of the likely consequences of withdrawing his consent. (3) An organisation must not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section does 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 must 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		disclosure (as the case may be) without the consent of the individual is required or authorised under this Act or other written law. **<u>Advisory Guidelines on Key Concepts in the PDPA (Consent Obligation)</u>** 12.41 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.

Qualifications to the Provision of Choice Mechanisms

The following are situations in which the application of the Global CBPR Choice Principle may not be necessary or practical.

i. **Obviousness:** Personal information controllers do not need to provide a mechanism for individuals to exercise choice in the collection, use or third-party sharing of personal information in those circumstances where consent by the individual can be inferred from the provision of the individual's information.

ii. **Collection of Publicly-Available Information**: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the collection and use of publicly available information.

iii. **Technological Impracticability**: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to those cases where electronic technology automatically collects information when a prospective customer initiates contact [e.g., use of cookies]. However, a mechanism to exercise choice as to use and disclosure should be provided after collection of the information.

iv. **Third-Party Receipt**: Where personal information is received from a third party, the recipient personal information controller does not need to provide a mechanism for individuals to exercise choice in relation to the collection of the information. However, if the personal information controller engages a third party to collect personal information on its behalf, the personal information controller should instruct the collector to provide such choice when collecting the personal information.

v. **Disclosure to a government institution which has made a request for the information with lawful authority**: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to disclosure to law enforcement agencies for investigation purposes where the provision of such mechanism to the individual will likely prejudice the investigation.

vi. **Disclosure to a third party pursuant to a lawful form of process:** Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.

vii. **For legitimate investigation purposes**: When providing a mechanism for individuals to exercise choice would compromise the availability or accuracy of the personal information and its collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.

viii. **Action in the event of an emergency**: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in emergency situations that threaten the life, health or security of an individual.

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 Privacy Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.*

Question	**Assessment Criteria**	**Enforceability - SINGAPORE** *Personal Data Protection Act 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 Organisation answers **YES**, the Accountability Agent must require the Applicant Organisation to provide the procedures the Applicant Organisation 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 Organisation to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use**. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation 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 Privacy Principle.	**Accuracy of personal data** 23. An organisation must 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. **Advisory Guidelines on Key Concepts in the PDPA (Accuracy Obligation)** 16.1 Section 23 of the PDPA requires an organisation to 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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
22. Do you have a mechanism for correcting inaccurate, incomplete and outdated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	Where the Applicant Organisation answers **YES**, the Accountability Agent must require the Applicant Organisation to provide the procedures and steps the Applicant Organisation has in place for correcting inaccurate, incomplete and outdated personal information, which includes, but is not 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 Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation 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 Privacy Principle.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned 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 must — (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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		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 (3) of a correction of personal data, the organisation must 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 must 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 requires 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 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 Organisation answers **YES**, the Accountability Agent must require the Applicant Organisation to provide the procedures the Applicant Organisation 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 Organisation's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant Organisation's behalf. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation 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 Privacy Principle.	**Application of the Act** 4.(2) Parts 3, 4, 5, 6 (except for sections 24 (protection of personal data) and section 25 (retention of personal data)), 6A (except sections 26C(3)(a) and 26E) and 6B do 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 has 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 must — (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

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		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 (3) of a correction of personal data, the organisation must 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 must 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 requires 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Accuracy of personal data</u> 23. An organisation must 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 the personal information was disclosed? If YES, describe.	Where the Applicant Organisation answers **YES**, the Accountability Agent must require the Applicant Organisation to provide the procedures the Applicant Organisation has in place to communicate corrections to other third parties, to whom personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this Privacy 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 must — (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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 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 must 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 must 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 requires 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. **<u>Accuracy of personal data</u>** 23. An organisation must make reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data –

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(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.
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 Organisation answers **YES**, the Accountability Agent must require the Applicant Organisation to provide the procedures the Applicant Organisation 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 Organisation 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 Organisation and by the processors, agents or other service providers. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation 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 Privacy principle.	**Application of the Act** 4(3). An organisation has 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 must 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 must make reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data –

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(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. **<u>Advisory Guidelines on Key Concepts in the PDPA (Accuracy Obligation)</u>** 16.7 An organisation should also be more careful when collecting personal data about an individual from a source other than the individual in question. It is allowed to take differing approaches to ascertain the accuracy and completeness of personal data it collects depending on the reliability of the source of the data. For example, the organisation may obtain confirmation from the source of the personal data that the source had verified the accuracy and completeness of that personal data. It may also conduct further independent verification if it deems prudent to do so.

SECURITY SAFEGUARDS

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

Question	**Assessment Criteria**	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
26. Have you implemented an information security policy?	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation that the implementation of a written information security policy is required for compliance with this Privacy Principle.	**Compliance with Act** 11.(1) In meeting its responsibilities under this Act, an organisation must 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 must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(ii) the complaint process mentioned in paragraph (b). **<u>Protection of personal data</u>** 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. **<u>Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)</u>** 17.1 Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. This obligation of organisations to protect personal data is referred to in these Guidelines as the Protection Obligation. 17.2 There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Each organisation should consider

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		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. For example, in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on.
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorised access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant Organisation 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 (e.g., password protections)** • **Encryption** • **Boundary protection (e.g., firewalls, intrusion detection)** • **Audit logging** • **Monitoring (e.g., external and internal audits, vulnerability scans)** • **Other (specify)** The Applicant Organisation must implement reasonable administrative, technical and physical safeguards, suitable to the	**Protection of personal data** 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. **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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	Applicant Organisation's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third-Party personal information it collects, in order to protect that information from leakage, loss or unauthorised 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 Organisation 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 unauthorised access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organisation must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant Organisation indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant Organisation that the implementation of such safeguards is required for compliance with this Privacy Principle.	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. 17.5 - Security arrangements may take various forms such as administrative measures, physical measures, technical measures or a combination of these. **<u>Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)</u>** 17.1 Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. This obligation of organisations to protect personal data is referred to in these Guidelines as the Protection Obligation. 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		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. For example, in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on. 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.
28. Describe how the safeguards you 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.	Where the Applicant Organisation provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified. The Applicant Organisation must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organisation'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	**<u>Compliance with Act</u>** 11.(1) In meeting its responsibilities under this Act, an organisation must 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	from unauthorised leakage, loss, use, alteration, disclosure, distribution, or access.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **Protection of personal data** 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 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. For example, in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on. 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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		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 so doing, 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.
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 Organisation'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, or • Other (specify). Where the Applicant Organisation 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 Organisation that the existence of such procedures are required for compliance with this Privacy Principle.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b).

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Protection of personal data</u> 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. **<u>Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)</u>** 17.3b – In practice, an organisation should identify reliable and well-trained personnel responsible for ensuring information security.
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	Where the Applicant Organisation 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 Organisation must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant Organisation answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant Organisation that the existence of safeguards on each category is required for compliance with this Privacy Principle.	**<u>Compliance with Act</u>** 11.(1) In meeting its responsibilities under this Act, an organisation must 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. **<u>Policies and practices</u>** 12. An organisation must –

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
network and software design, as well as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures? 30.d) Physical security?		(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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **Protection of personal data** 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. **Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)** 17.2 - There is no 'one size fits all' solution for organisations to comply with the Protection

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		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 Organisation answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform Applicant Organisation that the existence of a policy for the secure disposal of personal information is required for compliance with this Privacy Principle.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **<u>Protection of personal data</u>** 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant Organisation 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 Organisation answers **NO,** the Accountability Agent must inform the Applicant Organisation that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this Privacy Principle.	**<u>Policies and practices</u>** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(ii) the complaint process mentioned in paragraph (b). **<u>Protection of personal data</u>** 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.
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 Organisation adjusts their security safeguards to reflect the results of these tests.	**<u>Policies and practices</u>** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b).

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Protection of personal data</u> 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. **<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. 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 so doing, 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)

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		whether the personal data is or will be held or used by a third party on behalf of the organisation. **Guide to Data Protection Practices for ICT Systems** Page 27 - 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 **third- party certifications or other risk assessments**? Describe below.	The Accountability Agent must verify that such **risk assessments or certifications** are undertaken at appropriate intervals, and that the Applicant Organisation 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 Organisation and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	**Protection of personal data** 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. **Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)** 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;

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		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. **<u>Advisory Guidelines on Key Concepts in the PDPA (Accountability Obligation)</u>** 21.15 Although not expressly provided for in the PDPA, organisations may wish to consider demonstrating organisational accountability through measures such as conducting Data Protection Impact Assessments ("DPIA") in appropriate circumstances, adopting a Data Protection by Design ("DPbD") approach, or implementing a Data Protection Management Programme ("DPMP"), to ensure that their handling of personal data is in compliance with the PDPA. Although failing to undertake such measures is not itself a breach of the PDPA, it could, in certain circumstances, result in the organisation failing to meet other obligations under the PDPA.
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorised access, destruction, use, modification	The Accountability Agent must verify that the Applicant Organisation 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 unauthorised access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organisation must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	**<u>Application of the Act</u>** 4(2) Parts 3, 4, 5, 6 (except for sections 24 (protection of personal data) and section 25 (retention of personal data)), 6A (except sections 26C(3)(a) and 26E) and 6B do 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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the 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 Organisation's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?		4(3) An organisation has 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 must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **Protection of personal data** 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent —

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. **<u>Notifiable data breaches</u>** 26B.(1) A data breach is a notifiable data breach if the data breach — (a) results in, or is likely to result in, significant harm to an affected individual; or (b) is, or is likely to be, of a significant scale. **<u>Duty to conduct assessment of data breach</u>** 26C.(1) This section applies to a data breach that occurs on or after 1 February 2021. (2) Subject to subsection (3), where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach. (3) Where a data intermediary (other than a data intermediary mentioned in section 26E) has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation —

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(a) the data intermediary must, without undue delay, notify that other organisation of the occurrence of the data breach; and (b) that other organisation must, upon notification by the data intermediary, conduct an assessment of whether the data breach is a notifiable data breach. **Duty to notify occurrence of notifiable data breach** 26D.(1) Where an organisation assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must notify the Commission as soon as is practicable, but in any case no later than 3 calendar days after the day the organisation makes that assessment. **Transfer of personal data outside Singapore** 26.(1) An organisation must 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:

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		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.

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. The Qualifications to the Provision of Access and Correction Mechanisms are listed below and set 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.

Question	**Assessment Criteria**	**Enforceability - SINGAPORE** *Personal Data Protection Act 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 Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation has procedures in place to respond to such requests. The Applicant Organisation 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 Organisation'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. The personal information must be provided to individuals in an easily comprehensible way.	**<u>Access to personal data</u>** 21.(1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation must, 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 mentioned 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	The Applicant Organisation must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant Organisation answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organisation that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organisation identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	other information under subsection (1) in respect of the matters specified in the Fifth Schedule[39]. (3) An organisation must 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. (3A) Subsection (3)(c) and (d) does not apply to any user activity data about, or any user provided data from, the individual who made the request despite such data containing personal data about another individual. (4) An organisation must not inform any individual under subsection (1) that it has disclosed personal data to a prescribed

[39] PDPA Fifth Schedule – Exceptions from access requirement.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		law enforcement agency if the disclosure was made under this Act or under any other written law without the individual's consent. (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 must 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). **Fifth Schedule – Section 21(2) – Exceptions from access requirement** 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. **PERSONAL DATA PROTECTION REGULATIONS 2021** **Part II: Requests for access to and correction of personal data** **Duty to respond to request under section 21(1) of Act**

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		4.(1) Subject to section 21(2), (3), (3A) 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 on or after 1 February 2021 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 (as the case may be), 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 any of the following – (a) the existence of personal data mentioned in paragraph 1(h) of the Fifth Schedule to the Act as in force before, on or after 1 February 2021; (b) the use or disclosure of personal data without consent under the following provisions for any

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		investigation or proceedings, if the investigation or proceedings and related appeals have not been completed: (i) paragraph 3 of Part 3 of the First Schedule to the Act as in force on or after 1 February 2021; (ii) paragraph 1(e) of the Third Schedule to the Act or paragraph 1(f) of the Fourth Schedule to the Act (as the case may be) as in force before 1 February 2021.
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 Organisation'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. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe.	Where the Applicant Organisation answers **YES,** the Accountability Agent must verify each answer provided. The Applicant Organisation 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 Organisation 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 Organisation answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organisation that it may be required to permit access by individuals to their personal information. Where the Applicant Organisation identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	**<u>Access to personal data</u>** 21.(1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation must, 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 mentioned 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 Schedule42. (3) Subject to subsection (3A), an organisation must 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
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 interaction with the individual (e.g., email, same language, etc.)? 37.e) Do you charge a fee for providing access? If YES, describe below what the fee is based and how you ensure that the fee is not excessive.		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. (3A) Subsection (3)(c) and (d) does not apply to any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual. (4) An organisation must not inform any individual under subsection (1)(b) that the organisation has disclosed personal data about the individual to a prescribed law enforcement agency if the disclosure was made under this Act or any other written law without the individual's consent. (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 must provide the individual with access to the

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4). **PERSONAL DATA PROTECTION REGULATIONS 2021** **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), (3A) 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 on or after 1 February 2021 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 on or after 1 February 2021 – (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 (c) in such other form requested by the applicant as is acceptable to the organisation.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Notification of timeframe for response</u> 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 (as the case may be), 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. **<u>Refusal to confirm or deny existence, use or disclosure of personal data</u>** 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 any of the following – (a) the existence of personal data mentioned in paragraph 1(h) of the Fifth Schedule to the Act as in force before, on or after 1 February 2021; (b) the use or disclosure of personal data without consent under the following provisions for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed: (i) paragraph 3 of Part 3 of the First Schedule to the Act as in force on or after 1 February 2021;

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(ii) paragraph 1(e) of the Third Schedule to the Act or paragraph 1(f) of the Fourth Schedule to the Act (as the case may be) as in force before 1 February 2021. **<u>Fees</u>** 7.(1) Subject to section 28 of the Act as in force immediately before 1 February 2021 or section 48H of the Act (as the case may be), 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 —

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		(A) has reviewed the higher fee under section 28(1) of the Act as in force immediately before 1 February 2021, the fee allowed by the Commission under section 28(2) of the Act as in force immediately before that date; or (B) has reviewed the higher fee under section 48H(1) of the Act, the fee allowed by the Commission under section 48H(2) of the Act; or (ii) if sub-paragraph (i) does not apply, the higher fee notified under paragraph (2)(b); (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 — (A) has reviewed the estimated fee under section 28(1) of the Act as in force immediately before 1 February 2021, the fee allowed by the Commission under section 28(2) of the Act as in force immediately before that date; or (B) has reviewed the estimated fee under section 48H(1) of the Act, the fee allowed by the Commission under section 48H(2) of the Act; or (ii) if sub-paragraph (i) does not apply, the estimated fee provided under paragraph (2)(a). For the avoidance of doubt, an organisation must not charge the applicant any fee to comply with its obligations under section 22(2) of the Act.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts (Access and Correction Obligation)</u> <u>Obligation to provide access to personal data</u> 15.5 An organisation's obligation in responding to an access request is to provide the individual access to the personal data requested by the individual which is in the organisation's possession or under its control, unless any relevant exception in section 21 or the Fifth Schedule to the PDPA applies. 15.6 To be clear, an organisation is not required to provide access to the documents (or systems) which do not comprise or contain the personal data in question, so long as the organisation provides the individual with the personal data that the individual requested and is entitled to have access to under section 21 of the PDPA. In the case of a document containing the personal data in question, the organisation should, where feasible, provide only the personal data (or relevant sections of the document containing the personal data) without providing access to the entire document in its original form. 15.7 An organisation does not need to provide access to information which is no longer within its possession or under its control when the access request is received. The organisation should generally inform the requesting individual that it no longer possesses the personal data and is thus unable to meet the individual's access request.

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		Organisations are also not required to provide information on the source of the personal data. <u>Response time frame for an access request</u> 15.18 Subject to the PDPA and the Personal Data Protection Regulations 2021, an organisation is required to comply with section 21(1) of the PDPA and must respond to an access request as soon as reasonably possible from the time the access request is received. If an organisation is unable to respond to an access request within 30 days after receiving the request, the organisation shall inform the individual in writing within 30 days of the time by which it will be able to respond to the request. <u>Fees chargeable to comply with the access obligation</u> 15.25 An organisation may charge an individual a reasonable fee to process an access request by the individual. The purpose of the fee is to allow organisations to recover the incremental costs of responding to the access request. This may include the time and costs incurred to search for the personal data requested. An example of such incremental costs is the cost of producing a physical copy of the personal data for the individual requesting it. As organisations are required to make the necessary arrangements to provide for standard types of access requests, costs incurred in capital purchases (e.g. purchasing new equipment in order to provide access

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		to the requested personal data) should not be transferred to individuals. 15.26 The Commission is of the view that it would be difficult to prescribe a standard fee or range of fees at the outset to apply across all industries or all types of access requests. Organisations should exercise proper judgement in deriving the reasonable fee they charge based on their incremental costs of providing access. The Commission may, upon the application of an individual, review a fee charged by an organisation under section 48H of the PDPA (among other matters). In reviewing a fee, the Commission may consider the relevant circumstances, including the absolute amount of the fee, the incremental cost of providing access which may include the time and costs incurred to search for the personal data requested, and similar fees charged in the industry. 15.27 If an organisation wishes to charge an individual a fee to process an access request, the organisation must give the individual a written estimate of the fee. If the organisation wishes to charge a fee higher than the original written estimate, it must inform the individual in writing of the increased fee. The organisation may refuse to process or provide access to the individual's personal data until the individual agrees to pay the relevant fee.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
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 Organisation's policies/procedures in this regard below and answer questions 38 (a) – (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. 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?	Where the Applicant Organisation answers **YES to questions 38(a)**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant Organisation 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. 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 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 Organisation answers **NO** to questions 38(a) – (e) and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organisation that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organisation identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	**<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 must – (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 (3) of a correction of personal data, the organisation must 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.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the 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?		(5) If no correction is made under subsection (2)(a) or (4), the organisation must 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 requires 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. **Advisory Guidelines on Key Concepts (Access and Correct Obligation)** Obligation to correct personal data 15.45 Section 22(1) of the PDPA provides that an individual may submit a request for an organisation to correct an error or omission in the individual's personal data that is in the possession or under the control of the organisation (a "correction request"). Upon receipt of a correction request, the organisation is required to consider whether the correction should be made. In particular, section 22(2) goes on to provide that unless the organisation is satisfied on reasonable grounds that the correction should not be made, it should – a) correct the personal data as soon as practicable; and b) send the corrected personal data to every other organisation to which the personal data was

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		disclosed by the organisation within a year before the date the correction request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

Qualifications to the Provision of Access and Correction Mechanisms

Although organisations should always make good faith efforts to provide access, there are some situations, described below, in which it may be necessary for organisations to deny access requests. Please identify which, if any, of these situations apply, and specify their application to you, with reference to your responses provided to the previous questions, in the space provided.

i. **Disproportionate Burden:** Personal information controllers do not need to provide access and correction where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, as for example when claims for access are repetitious or vexatious by nature.

ii. **Protection of Confidential Information:** Personal information controllers do not need to provide access and correction where the information cannot be disclosed due to legal or security reasons or to protect confidential commercial information (i.e., information that you have taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against your business interest causing significant financial loss). Where confidential commercial information can be readily separated from other information subject to an access request, the personal information controller should redact the confidential commercial information and make available the non-confidential commercial information to the extent that such information constitutes personal information of the individual concerned. Other situations would include those where disclosure of information would benefit a competitor in the market place, such as a particular computer or modeling program. Furthermore, a denial of access may also be considered acceptable in situations where, for example providing the information would constitute a violation of laws or would compromise security.

iii. **Third Party Risk:** Personal information controllers do not need to provide access and correction where the information privacy of persons other than the individual would be violated. In those instances where a third party's personal information can be severed from the information requested for access or correction, the personal information controller must release the information after redaction of the third party's personal information.

ACCOUNTABILITY

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant Organisation is accountable for complying with measures that give effect to the other Privacy Principles stated above. Additionally, when transferring information, the Applicant Organisation should be accountable for ensuring that the recipient will protect the information consistently with these Privacy Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Privacy 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 Privacy Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question	**Assessment Criteria**	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
39. What measures do you take to ensure compliance with the Global CBPR 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 Organisation indicates the measures it takes to ensure compliance with the Global CBPR Privacy Principles. Where the Applicant Organisation answers it does not maintain records of processing activities, the Accountability Agent must inform the Applicant Organisation that it must have procedures in place to maintain records of processing activities.	**<u>Application of the Act</u>** 4.(6) Unless otherwise expressly provided in this Act – (a) nothing in Parts 3, 4, 5, 6, 6A and 6B affects 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 is not an excuse for contravening this Act; and (b) the provisions of other written law prevail to the extent that any provision of Parts 3, 4, 5, 6, 6A and 6B is inconsistent with the provisions of that other written law.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
• Compliance with self-regulatory Applicant Organisation code and/or rules _____ • Other (describe) __		**<u>Compliance with Act</u>** 11.(1) In meeting its responsibilities under this Act, an organisation must 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. **<u>Policies and practices</u>** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b).

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts (Accountability Obligation)</u> 21.1 In data protection, the concept of accountability refers to how an organisation discharges its responsibility for personal data in its possession or which it has control over81. This may include situations where the organisation can determine the purposes for which the personal data is collected, used or disclosed, or the manner and means by which the data is processed. This general concept of accountability is in Part 3 of the PDPA on "General Rules with Respect to Protection of and Accountability for Personal Data" and premised on section 11(2) within Part 3 of the PDPA, which states, "An organisation is responsible for personal data in its possession or under its control.". 21.2 Accountability under the PDPA requires organisations to undertake measures in order to ensure that they meet their obligations under the PDPA and, importantly, demonstrate that they can do so when required. Some of these measures are specifically required under the PDPA. For example, designating one or more individuals to be responsible for ensuring the organisation's compliance with the PDPA, developing and implementing policies and practices that are necessary for the organisation to meet its obligations under the PDPA ("data protection policies and practices"), and making

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		information about their data protection policies and practices available.
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Global CBPR Privacy Principles?	Where the Applicant Organisation answers **YES,** the Accountability Agent must verify that the Applicant Organisation has designated an employee(s) who is responsible for the Applicant Organisation's overall compliance with these Privacy Principles. The Applicant Organisation must designate an individual or individuals to be responsible for the Applicant Organisation'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. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation that designation of such an employee(s) is required for compliance with this Privacy Principle.	**<u>Compliance with Act</u>** 11.(1) In meeting its responsibilities under this Act, an organisation must 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 must designate one or more individuals to be responsible for ensuring that the organisation complies with this Act. **<u>Advisory Guidelines on Key Concepts in the PDPA (Accountability Obligation)</u>** 21.3 Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA. This individual is typically referred to as a DPO. Section 11(4) further provides that an individual so designated by an organisation may delegate the responsibility conferred by that designation to another individual. Section 11(6) clarifies that the designation of an individual by an organisation under section 11(3) does not relieve the organisation of any of its obligations under the

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		PDPA. That is, legal responsibility for complying with the PDPA remains with the organisation and is not transferred to the designated individual(s). On the whole, these provisions require organisations to designate the appropriate individuals, who may in turn delegate certain responsibilities to other officers, so that collectively, they co-operate to ensure that the organisation complies with the PDPA. 21.4 An organisation's DPO plays an essential role in how the organisation meets its obligations under the PDPA. The responsibilities of the DPO often include working with senior management and the organisation's business units to develop and implement appropriate data protection policies and practices for the organisation. In addition, the DPO would undertake a wide range of activities, which may include producing (or guiding the production of) a personal data inventory, conducting data protection impact assessments, monitoring and reporting data protection risks, providing internal training on data protection compliance, engaging with stakeholders on data protection matters and generally acting as the primary internal expert on data protection. Depending on the organisation's needs, the DPO may also work with (or have additional responsibilities relating to) the organisation's data governance and cybersecurity functions. The DPO can also play a role in supporting an organisation's innovation.

Question	**Assessment Criteria**	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		21.5 Individual(s) designated by an organisation under section 11(3) should be: (a) sufficiently skilled and knowledgeable; and (b) amply empowered, to discharge their duties as a DPO, although they need not be an employee of the organisation. Organisations should ensure that individuals appointed as a DPO are trained and certified. The individual(s) should ideally be a member of the organisation's senior management team or have a direct reporting line to the senior management to ensure the effective development and implementation of the organisation's data protection policies and practices. As part of corporate governance, the commitment and involvement of senior management is key to ensure that there is accountability and oversight over the management of personal data in the organisation.
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant Organisation answers **YES,** the Accountability Agent must verify that the Applicant Organisation 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 Organisation (e.g., Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant Organisation's compliance with the Global CBPR Framework and/or requests from	**<u>Policies and practices</u>** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about –

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation that implementation of such procedures is required for compliance with this Privacy Principle.	(i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **<u>Advisory Guidelines on Key Concepts in the PDPA (Accountability Obligation)</u>** 21.10 Secondly, an organisation must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA. This is to ensure that the organisation can effectively address individuals' complaints and concerns with its data protection policies and practices and aid in its overall compliance efforts. 21.12 Finally, an organisation is required to make information available on request concerning its data protection policies and practices and its complaint process. This is to ensure that individuals are able to find the necessary information and, if necessary, have the means of raising any concerns or complaints to the organisation directly.
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant Organisation answers **YES,** the Accountability Agent must verify that the Applicant Organisation has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation that implementation	**<u>Policies and practices</u>** 12. An organisation must – (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
	of such procedures is required for compliance with this Privacy 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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **<u>Advisory Guidelines on Key Concepts in the PDPA (Accountability Obligation)</u>** 21.7 - The business contact information of the relevant person may be provided on BizFile+ for companies that are registered with ACRA, or provided in a readily accessible part of the organisation's official website such that it can be easily found. It 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		21.10 Secondly, an organisation must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA. This is to ensure that the organisation can effectively address individuals' complaints and concerns with its data protection policies and practices and aid in its overall compliance efforts.
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 Organisation indicates what remedial action is considered.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b).

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts in the PDPA (Accountability Obligation)</u> 21.7 - The business contact information of the relevant person may be provided on BizFile+ for companies that are registered with ACRA, or provided in a readily accessible part of the organisation's official website such that it can be easily found. It 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. 21.10 Secondly, an organisation must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA. This is to ensure that the organisation can effectively address individuals' complaints and concerns with its data protection policies and practices and aid in its overall compliance efforts. 21.12 Finally, an organisation is required to make information available on request concerning its data protection policies and practices and its complaint process. This is to ensure that individuals are able to find the necessary information and, if necessary, have

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		the means of raising any concerns or complaints to the organisation directly.
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant Organisation 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 Organisation that the existence of such procedures is required for compliance with this Privacy Principle.	**Policies and practices** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **Advisory Guidelines on Key Concepts in the PDPA (Accountability Obligation)** 21.11 Thirdly, an organisation is required to provide staff training and communicate to its staff information about its policies and practices. Such communication efforts could be incorporated in organisations' training and awareness programmes and should include any additional information which may be

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		necessary for the organisation's staff to effectively implement its data protection policies and practices. An effective training and awareness programme builds a staff culture that is sensitive and alert to data protection issues and concerns.
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 Organisation answers **YES,** the Accountability Agent must verify that the Applicant Organisation 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 Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation that such procedures are required for compliance with this Privacy Principle.	**Application of the Act** 4.(6) Unless otherwise expressly provided in this Act – (a) nothing in Parts 3, 4, 5, 6, 6A and 6B affects 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 is not an excuse for contravening this Act; and (b) the provisions of other written law prevail to the extent that any provision of Parts 3, 4, 5, 6, 6A and 6B is inconsistent with the provisions of that other written law. **Compliance with Act** 11.(1) In meeting its responsibilities under this Act, an organisation must 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Policies and practices</u> 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **<u>Collection, use and disclosure without consent</u>** 17.(1) An organisation may collect personal data about an individual, without the individual's consent or from a source other than the individual, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 1 of the Second Schedule. (2) Unless otherwise provided under this Act, an organisation may —

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(a) collect personal data about an individual that the organisation receives by way of a disclosure to the organisation — (i) on or after 1 February 2021 in accordance with subsection (1)(c); or (ii) before 1 February 2021 in accordance with section 17(3) as in force before that date, for purposes consistent with the purpose of that disclosure, or for any purpose permitted by subsection (1)(a); or (b) use or disclose personal data about an individual that — (i) is collected by the organisation on or after 1 February 2021 in accordance with subsection (1)(a); or (ii) was collected by the organisation before 1 February 2021 in accordance with section 17(1) as in force before that date, for purposes consistent with the purpose of that collection, or for any purpose permitted by subsection (1)(b) or (c), as the case may be. **ASEAN Model Contractual Clauses for Cross Border Data Flows** 3.11. The Data Importer shall promptly notify and consult with the Data Exporter regarding any investigation regarding the collection, use, transfer, disclosure, security, or disposal of the Personal Data

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		transferred under this contract, unless otherwise prohibited under law.
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 _____ • Compliance with self-regulatory Applicant Organisation code and/or rules _____ • Others (describe) _____	Where the Applicant Organisation answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation that implementation of such agreements is required for compliance with this Privacy Principle.	**Application of Act** 4.(2) Parts 3, 4, 5, 6 (except for sections 24 (protection of personal data) and section 25 (retention of personal data)), 6A (except sections 26C(3)(a) and 26E) and 6B do 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 has 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 must 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Policies and practices</u> 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **<u>Guide on data protection clauses for agreements relating to processing of personal data</u>** 2.1 - <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] 2.2 - <u>Process, use and disclosure</u>: The Contractor shall only process, use or disclose Customer Personal Data:

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(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 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,	The Accountability Agent must verify that the Applicant Organisation makes use of appropriate methods to ensure their obligations are met.	**<u>Application of Act</u>** 4.(2) Parts 3, 4, 5, 6 (except for sections 24 (protection of personal data) and section 25 (retention of personal data)), 6A (except sections

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
agents, contractors or other service providers: • Abide by your Global CBPR- compliant privacy policies and 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? • Be Global CBPR-certified by a Forum-		26C(3)(a) and 26E) and 6B do 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 has 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 must 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 must – (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
recognized Accountability Agent in their jurisdiction? _____ • Notify the Applicant Organisation in the case of a breach of the personal information of the Applicant Organisation's customers? • Other (describe) _		(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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **<u>Duty to conduct assessment of data breach</u>** 26C.—(1) This section applies to a data breach that occurs on or after 1 February 2021. (2) Subject to subsection (3), where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach. (3) Where a data intermediary (other than a data intermediary mentioned in section 26E) has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation —

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(a) the data intermediary must, without undue delay, notify that other organisation of the occurrence of the data breach; and (b) that other organisation must, upon notification by the data intermediary, conduct an assessment of whether the data breach is a notifiable data breach. **<u>Guide on data protection clauses for agreements relating to processing of personal data</u>** 2.1 - <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] 2.2 - <u>Process, use and disclosure</u>: The Contractor shall only process, use or 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

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		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]
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 3, 4, 5, 6 (except for sections 24 (protection of personal data) and section 25 (retention of personal data)), 6A (except sections 26C(3)(a) and 26E) and 6B do 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 has the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		if the personal data were processed by the organisation itself. **<u>Compliance with Act</u>** 11.-(1) In meeting its responsibilities under this Act, an organisation must 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. **<u>Policies and practices</u>** 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(ii) the complaint process mentioned in paragraph (b). **<u>Advisory Guidelines on Key Concepts in the PDPA</u>** <u>Obligations of data intermediaries</u> 6.16 The PDPA provides that a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the Data Protection Provisions relating to (a) protection of personal data (later referred to as the "Protection Obligation"); (b) retention of personal data (later referred to as the "Retention Limitation Obligation"); and (c) notifying the organisation of data breaches as part of notification of data breaches (later referred to as the "Data Breach Notification Obligation"), and not any of the other Data Protection Provisions. <u>Considerations for organisations using data intermediaries</u> 6.20 Section 4(3) provides that an organisation has the same obligations under the PDPA in respect of personal data processed on its behalf by a data intermediary as if the personal data were processed

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		by the organisation itself. As such, it is good practice for an organisation to undertake an appropriate level of due diligence to assure itself that a potential data intermediary is capable of complying with the PDPA. 6.21 When engaging a data intermediary, an organisation should make clear in its contract the scope of work that the data intermediary is to perform on its behalf and for its purposes. For instance, if the organisation requires the data intermediary to process personal data on its behalf to respond to access or correction requests by individuals, the organisation should include contractual clauses to ensure that the data intermediary's scope of work and level of responsibilities are clear. The data intermediary has independent obligations to protect and cease retention of personal data that it has received for processing under the contract. Where a data breach is discovered by a data intermediary that is processing personal data on behalf and for the purposes of another organisation, the data intermediary is required to notify the organisation without undue delay from the time it has credible grounds to believe that the data breach has occurred. The organisation remains liable for any breach of the Data Protection Provisions for any processing by a data intermediary on its behalf and for its purposes.

Question	Assessment Criteria	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		Accountability Obligation 21.15 Although not expressly provided for in the PDPA, organisations may wish to consider demonstrating organisational accountability through measures such as conducting Data Protection Impact Assessments ("DPIA") in appropriate circumstances, adopting a Data Protection by Design ("DPbD") approach, or implementing a Data Protection Management Programme ("DPMP"), to ensure that their handling of personal data is in compliance with the PDPA92. Although failing to undertake such measures is not itself a breach of the PDPA, it could, in certain circumstances, result in the organisation failing to meet other obligations under the PDPA. **Guide to Managing Data Intermediaries** Page 24 - There may be circumstances where a Data Controller (DC) would like to verify that its Data Intermediary (DI) is properly carrying out its roles and responsibilities, particularly where the DI is involved in processing large amounts of sensitive personal data over long periods. In such cases, the DC could consider conducting audit exercises, requesting an independent audit report or having onsite inspections at the DI's premises. The necessity and frequency of audits and on-site inspections will be determined by the risk profile of the DC, the nature and extent of data processing activities

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		outsourced, and the severity and likelihood of occurrence of the risks identified. Audit remediation measures are also critical in ensuring that any data protection risks are addressed effectively.
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify the existence of the Applicant Organisation's procedures such as spot checking or monitoring mechanisms. Where the Applicant Organisation answers **NO**, the Accountability Agent must require the Applicant Organisation to describe why it does not make use of such spot checking or monitoring mechanisms.	**Application of Act** 4.(2) Parts 3, 4, 5, 6 (except for sections 24 (protection of personal data) and section 25 (retention of personal data)), 6A (except sections 26C(3)(a) and 26E) and 6B do 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 has 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. **Advisory Guidelines on Key Concepts in the PDPA** Considerations for organisations using data intermediaries 6.20 Section 4(3) provides that an organisation has the same obligations under the PDPA in respect of personal data processed on its behalf by a data intermediary as if the personal data were processed by

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		the organisation itself. As such, it is good practice for an organisation to undertake an appropriate level of due diligence to assure itself that a potential data intermediary is capable of complying with the PDPA. 6.21 When engaging a data intermediary, an organisation should make clear in its contract the scope of work that the data intermediary is to perform on its behalf and for its purposes. For instance, if the organisation requires the data intermediary to process personal data on its behalf to respond to access or correction requests by individuals, the organisation should include contractual clauses to ensure that the data intermediary's scope of work and level of responsibilities are clear. The data intermediary has independent obligations to protect and cease retention of personal data that it has received for processing under the contract. Where a data breach is discovered by a data intermediary that is processing personal data on behalf and for the purposes of another organisation, the data intermediary is required to notify the organisation without undue delay from the time it has credible grounds to believe that the data breach has occurred. The organisation remains liable for any breach of the Data Protection Provisions for any processing by a data intermediary on its behalf and for its purposes.

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Guide to Managing Data Intermediaries</u> Page 18 - Another role of the Data Controller (DC) is to define the format (e.g. level of detail required) and frequency (e.g. daily, weekly, ad-hoc) of the reports from its Data Intermediary (DI). i. Regular management report Management reports should be surfaced regularly to provide the DC's management with the information to monitor and manage business operations. Such regular reports help to ensure effective management of DIs. ii. Ad-hoc incident report Incident reports are surfaced based on issues that require special attention, such as a data incident. In this regard, the DC should have in place an escalation process and a reporting chain for incident reporting to ensure DIs notify them without undue delay when DIs become aware of any data incidents. SOPs should also cover incident investigation and management, and data breach notification procedures. Additionally, in the event of a data breach, DCs should put in place drawer plans for data breach management for their DIs to take remedial actions to address the data breach. Page 24 - There may be circumstances where a DC would like to verify that its DI is properly carrying out its roles and responsibilities, particularly where the DI

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		is involved in processing large amounts of sensitive personal data over long periods. In such cases, the DC could consider conducting audit exercises, requesting an independent audit report or having onsite inspections at the DI's premises. The necessity and frequency of audits and on-site inspections will be determined by the risk profile of the DC, the nature and extent of data processing activities outsourced, and the severity and likelihood of occurrence of the risks identified. Audit remediation measures are also critical in ensuring that any data protection risks are addressed effectively. **<u>Compliance with Act</u>** 11.(1) In meeting its responsibilities under this Act, an organisation must 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. **<u>Policies and practices</u>** 12. An organisation must – (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		(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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **<u>Guide to Managing Data Intermediaries</u>** Page 24 - There may be circumstances where a Data Controller (DC) would like to verify that its Data Intermediary (DI) is properly carrying out its roles and responsibilities, particularly where the DI is involved in processing large amounts of sensitive personal data over long periods. In such cases, the DC could consider conducting audit exercises, requesting an independent audit report or having onsite inspections at the DI's premises. The necessity and frequency of audits and on-site inspections will be determined by the risk profile of the DC, the nature and extent of data processing activities outsourced, and the severity and likelihood of occurrence of the risks identified. Audit remediation measures are also

Question	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		critical in ensuring that any data protection risks are addressed effectively.
50. Do you disclose personal information to other recipient **persons or organisations** in situations where due diligence and reasonable steps to ensure compliance with the Global CBPR System by the recipient as described above is impractical or impossible?	If **YES**, the Accountability Agent must ask the Applicant Organisation 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 Organisation for ensuring that the information, nevertheless, is protected consistent with the Global CBPR Privacy Principles. Where the Applicant Organisation relies on an individual's consent, the Applicant Organisation must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	**Application of Act** 4.(2) Parts 3, 4, 5, 6 (except for sections 24 (protection of personal data) and section 25 (retention of personal data)), 6A (except sections 26C(3)(a) and 26E) and 6B do 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 has 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 must 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	Assessment Criteria	Enforceability - SINGAPORE *Personal Data Protection Act 2012*
		<u>Policies and practices</u> 12. An organisation must – (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 mentioned in paragraph (a); and (d) make information available on request about – (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b). **<u>Protection of personal data</u>** 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.