Annex C[1]

GLOBAL PRIVACY RECOGNTION FOR PROCESSORS 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 Privacy Recognition for Processors (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 PRP System Program Requirements to guide an Applicant's explanation of how each 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 PRP 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. Additional documentation to assist in these explanations may be submitted as necessary.

Contents

[1] Annex C does 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.

SECURITY SAFEGUARDS

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
1. Has your organisation implemented an information security policy that covers personal information processed on behalf of a controller?	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.	**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 ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
2. Describe the physical, technical and administrative safeguards that implement your organisation's information security policy.	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 periodically review and reassess these 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.	**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; 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.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
3. Describe how your organisation makes employees aware of the importance of maintaining the security of personal information.	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 • 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 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). **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 ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		<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. **(Accountability Obligation)** 21.11 An organisation is required to provide staff training and communicate to its staff information about its policies and practices[2]. Such communication efforts could be incorporated in organisations' training and awareness programmes and should include any additional information which may be 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.
4. Has your organisation implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?	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 related to personal information. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant that the existence of such measures 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

[2] Section 12(c) of the PDPA.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**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.
5. Does your organisation have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.	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. 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 *(to be answered by the Applicant Organisation)*	Assessment Criteria *(to be verified by the Accountability Agent)*	**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 sensitivities; and d) be prepared and able to respond to information security breaches promptly and effectively. 17.4 - In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. In doing so, the following factors may be considered: a) the size of the organisation and the amount and type of personal data it holds;

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**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>Guide to Data Protection Practices for ICT Systems</u>** 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.
6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organisation's personal information?	The Accountability Agent must verify that the Applicant Organisation has in place appropriate processes to notify the controller of occurrences of a breach of the privacy or security of their organisation's personal information.	**<u>Data Breach Notification</u>** 26C. (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 — (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.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts in the PDPA (Data Breach Notification Obligation)</u> 20.7 Where a data breach is discovered by a data intermediary that is processing personal data on behalf and for the purposes of another organisation or public agency, the data intermediary is required to notify the organisation or public agency without undue delay from the time it has credible grounds to believe that the data breach has occurred. This ensures the organisation is (a) informed of data breaches in a timely way; (b) able to decide on the immediate actions to take to contain the data breach; and (c) able to assess whether the data breach is a notifiable data breach.
7. Has your organisation implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify the existence of procedures for the secure disposal or return of personal information. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures 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 (ii) the complaint process mentioned in paragraph (b).

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**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>Retention of personal data</u>** 25. An organisation must cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that — (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and (b) retention is no longer necessary for legal or business purposes.
8. Does your organisation use third-party certifications or other risk assessments? Please describe.	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.	**<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.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)</u> 17.4 In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their 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. **<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.

ACCOUNTABILITY MEASURES

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
9. Does your organisation limit its processing of personal information to the purposes specified by the controller?	The Accountability Agent must verify that the Applicant Organisation has policies in place to limit its processing to the purposes specified by the controller.	**<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>Retention of personal data</u>** 25. An organisation must cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that – (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and (b) the retention is no longer necessary for legal or business purposes.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
10. Does your organisation have procedures in place to delete, update, and correct information upon request from the controller?	The Accountability Agent must verify that the Applicant Organisation has measures in place to delete, update, and correct information upon request from the controller where necessary and appropriate.	**<u>Withdrawal of consent</u>** 16(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 other written law. **<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 the year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**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>Sixth Schedule - Section 22(7) - Exceptions from correction requirement</u>** 1. Section 22 does not apply in respect of — (a) opinion data kept solely for an evaluative purpose;

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		(b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results; (c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust; (d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; (e) a document related to a prosecution if all proceedings related to the prosecution have not been completed; or (f) derived personal data. **<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.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		<u>Retention of personal data</u> 25. An organisation must cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that – (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and (b) retention is no longer necessary for legal or business purposes.
11. What measures does your organisation take to ensure compliance with the controller's instructions related to the activities of personal information processing? Please describe.	The Accountability Agent must verify that the Applicant Organisation indicates the measures it takes to ensure compliance with the controller's instructions.	**<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>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

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**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).
12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the Global PRP System?	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 the Global PRP System. 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 the Global PRP System.	**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. **Advisory Guidelines on Key Concepts in the PDPA (Accountability Obligation)** 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.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		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 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 ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**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.
13. Does your organisation have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to handle, or forward to the controller as appropriate, privacy-related complaints or requests. 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.	**<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 ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		(i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b).
14. Does your organisation notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders 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 notifying the controller, except where prohibited by law, of judicial or other government subpoenas, warrants or orders 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.	**<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.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		<u>Guide on data protection clauses for agreements relating to the processing of personal data</u> 2.1 - Compliance with PDPA: The Contractor shall comply with all its obligations under the PDPA at its own cost. **<u>ASEAN Model Contractual Clauses for Cross Border Data Flows</u>** 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 transferred under this contract, unless otherwise prohibited under law. 2.2 - Process, use and disclosure: The Contractor shall only process, use and disclose Customer Personal Data: (a) strictly for the purposes of [fulfilling its obligations and providing the services required] under this Agreement; (b) with the Customer's prior written consent; or (c) when required by law or an order of court, but shall notify the Customer as soon as practicable before complying with such law or order of court at its own costs.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		[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.]
15. Does your organisation have a procedure in place to notify the controller of your engagement of subprocessors?	The Accountability Agent must verify that the Applicant Organisation has in place a procedure to notify controllers that the Applicant Organisation is engaging subprocessors.	**<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 ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		(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. **<u>Guide to Managing Data Intermediaries</u>** Page 33 – Data Controllers (DCs) may consider the following factors when negotiating contracts with Data Intermediaries (DIs): Polices and Practices c. prohibition of sub-contracting or requirement of the DC's approval before sub-contracting data processing activities that the DI is engaged to provide; d. where sub-contracting is allowed by the DC, the DI's agreement with the sub-contractor should impose the same obligations in relation to processing on the sub-contractor as imposed on the DI by the DC;

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)</u> 17.4 In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their 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.
16. Does your organisation have mechanisms in place with subprocessors to ensure that personal information is processed in accordance with your obligations under the Global PRP System? Please describe.	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify the existence of each type of mechanism described. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation that implementation of such mechanisms is required for compliance with this Privacy Principle.	**<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>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;

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		(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 33 – Data Controllers (DCs) may consider the following factors when negotiating contracts with Data Intermediaries (DIs): Polices and Practices c. prohibition of sub-contracting or requirement of the DC's approval before sub-contracting data processing activities that the DI is engaged to provide; d. where sub-contracting is allowed by the DC, the DI's agreement with the sub-contractor should impose the same obligations in relation to processing on the sub-contractor as imposed on the DI by the DC; **<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.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts in the PDPA (Protection Obligation)</u> 17.4 - In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their 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. **<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 transferred that is comparable to the protection under this Act.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts in the PDPA (Transfer Limitation Obligation)</u> 19.1 Section 26 of the PDPA limits the ability of organisations to transfer personal data to another organisation outside Singapore in circumstances where it relinquishes possession or direct control over the personal data. Such circumstances include transferring personal data to another company within the same group for centralized corporate functions, or to a data intermediary for data processing. In suituations where personal data transferred or situated overseas remains in the possession or control of an organisation, the organisation has to comply with all the Data Protection Provisions. Such situations include where an employee travels overseas with customer lists on his notebook an organisation owns or leases and operates a warehouse overseas for archival of customer records; or an organisation stores personal data in an overseas data centre on servers that it owns and directly maintains. In these examples, the organisation has direct primary obligations under the Data Protection Provisions to, inter alia, protect the personal data, give effect to access and correction requests, and include these overseas data repositories in its data retention policy.
17. Do the mechanisms referred to above generally require that subprocessors:	The Accountability Agent must verify that the Applicant Organisation makes use of appropriate methods to ensure their obligations are met.	**<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 ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
a) Follow instructions provided by your organisation relating to the manner in which personal information must be handled? b) Impose restrictions on further subprocessing? c) Be Global PRP-certified by a Global CBPR Forum-recognized Accountability Agent in their jurisdiction? d) Provide your organisation with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts? If **YES**, describe. e) Allow your organisation to carry out regular spot checking or other monitoring activities? If **YES**, describe. f) 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>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;

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivities; and d) be prepared and able to respond to information security breaches promptly and effectively. 17.4 - In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. In 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. **<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 transferred that is comparable to the protection under this Act.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts in the PDPA (Transfer Limitation Obligation)</u> 19.1 Section 26 of the PDPA limits the ability of organisations to transfer personal data to another organisation outside Singapore in circumstances where it relinquishes possession or direct control over the personal data. Such circumstances include transferring personal data to another company within the same group for centralized corporate functions, or to a data intermediary for data processing. In suituations where personal data transferred or situated overseas remains in the possession or control of an organisation, the organisation has to comply with all the Data Protection Provisions. Such situations include where an employee travels overseas with customer lists on his notebook an organisation owns or leases and operates a warehouse overseas for archival of customer records; or an organisation stores personal data in an overseas data centre on servers that it owns and directly maintains. In these examples, the organisation has direct primary obligations under the Data Protection Provisions to, inter alia, protect the personal data, give effect to access and correction requests, and include these overseas data repositories in its data retention policy.

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		19.2 This is because the Transfer Limitation Obligation is a manifestation of the Accountability Obligation. When an organisation discloses personal data to another organisation, and both are in Singapore, the receiving organisation is subject to the PDPA and has to protect the personal data that it thereby receives. Likewise, when an organisation discloses personal data to its data intermediary, and both are in Singapore, the data intermediary is subject to the Protection, Retention Limitation and Data Breach Notification Obligations for the personal data that it thereby receives. However, when an organisation transfers personal data to another organisation that is outside Singapore (for example, a data intermediary or another company in the same group), the recipient organisation is not subject to the PDPA. The Accountability Obligation requires that the transferring organisation takes steps to ensure that the recipient organisation will continue to protect the personal data that it has received to a standard that is comparable to that established in PDPA. This is the *raison d'etre* for the Transfer Limitation Obligation. **<u>Guide to Managing Data Intermediaries</u>** Page 33 – Data Controllers (DCs) may consider the following factors when negotiating contracts with Data Intermediaries (DIs): Polices and Practices

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		g. where there is overseas transfer of personal data, consider i) the overseas locations where the personal data will be transferred; and (ii) the standard of protection for the transferred personal data, such that the DI only transfers to overseas locations with comparable data protection regimes, or the recipient is bound by legally enforceable obligations to ensure a comparable standard of protection.
18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.	Where the Applicant Organisation answers **YES**, the Accountability Agent must verify that the Applicant Organisation has procedures in place for training employees relating to personal information management and the controller's instructions. Where the Applicant Organisation answers **NO**, the Accountability Agent must inform the Applicant Organisation that the existence of such procedures 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 (ii) the complaint process mentioned in paragraph (b).

Question ***(to be answered by the Applicant Organisation)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability - SINGAPORE** *Personal Data Protection Act 2012*
		<u>Advisory Guidelines on Key Concepts in the PDPA (Accountability Obligation)</u> 21.11 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 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.