Schellman
APEC CBPR Accountability Agent Recertification Application

Table of Contents

Introduction

1. Schellman Compliance, LLC ("Schellman") is headquartered in the United States, Tampa, Florida. Schellman Compliance, LLC was formed as a Delaware limited liability company on approximately August 24, 2021. Schellman Compliance, LLC which is partly and indirectly owned by current or former Schellman & Company, LLC principals, directors, and executives, operates in an alternative practice structure with Schellman & Company, LLC. Schellman is also a PCI QSA, ISO certification body, FedRAMP 3rd Party Assessment Organization (3PAO) and current APEC Accountability Agent. Schellman provides compliance and certification services to a variety of companies, including PCI-DSS and PA-DSS assessments, FedRAMP assessments, HITRUST assessments, AICPA examinations (SOC 1, SOC 2, SOC 3), Penetration Testing services, ISO 27001, 27701, 9001, 20000, and 22301 certifications, GDPR, CCPA and MS DPR examinations, and several other types of compliance assessments.

Conflicts of Interest

2. Schellman decisions, as an Accountability Agent, are based on objective evidence of conformity, or non-conformity, obtained by Schellman; decisions are not influenced by other interests or by other parties. Management is committed to impartiality in every manner of the certification services.

3. Schellman is aware that threats to impartiality may include, but not be limited to, any of the following.

   3.1. Self-interest threats: threats that arise from a person or body acting in their own interest. A concern related to certification, as a threat to impartiality, is financial self-interest.

   3.2. Self-review threats: threats that arise from a person or body reviewing the work done by themselves. Auditing the program requirements of an Applicant organization or Participant organization to whom Schellman provided consultancy would be a self-review threat.

   3.3. Familiarity (or trust) threats: threats that arise from a person or body being too familiar with or trusting of another person instead of seeking audit evidence.

   3.4. Intimidation threats: threats that arise from a person or body having a perception of being coerced openly or secretively, such as a threat to be replaced or reported to a supervisor.

4. Schellman performs an annual Independence Review which helps to identify, analyze and document the possibilities for conflict of interests arising from provision of certification, including any conflicts arising from its relationships. Having relationships does not necessarily present Schellman with a conflict of interest; however, if any relationship creates a threat to impartiality, Schellman shall

document and be able to demonstrate how it eliminates or minimizes such threats as a result of the annual Independence Review.

5. As part of the Independence Review, each employee is required to disclose personal relationships with the management or owners of any Applicant organization or Participant organization on an annual basis. Additionally, Schellman shall evaluate its finances and sources of income and demonstrate that on an ongoing basis, commercial, financial or other pressures do not compromise its impartiality. The results of the review are reviewed by human resources and management and potential conflicts are analyzed at that time. Threats identified as a result of the Independence Review that could impact the impartiality of the services provided by Schellman will be handled on a per-incident basis and where appropriate, Schellman will withdraw from the engagement.

6. Note that a relationship that threatens the impartiality of Schellman can be based on ownership, governance, management, personnel, shared resources, finances, contracts, marketing and payment of a sales commission or other inducement for the referral of new clients, etc.

Outsourcing

7. Schellman does not outsource any activities related to the certification services that it provides. All related certification services activities are performed by Schellman employees.

8. The decision for granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing certification is not outsourced and is the sole responsibility of Schellman. Schellman is responsible for, and retains authority for, its decisions relating to certification services.

Key Elements of Independence for Certification Clients

9. Schellman will not offer or provide consulting or technical services related to the development or implementation of Participant organization's or Applicant organization's data privacy practices and procedures.

10. Schellman will not offer or provide internal audits to its certified clients.

11. Personnel handling sales for Schellman that may collect a sales commission will not be part of the certification audit team for an Applicant organization or Participant organization.

12. Schellman will not offer consulting or technical services related to the development of its privacy notice or statement or to its security safeguards.

13. Schellman will require personnel to reveal any situation known to them that may present them or Schellman with a conflict of interest. Schellman will use this information as input to identifying threats to impartiality raised by the activities of such personnel or by the organizations that employ them, and shall not use such personnel, internal or external, unless they can demonstrate that there is no conflict of interest. If a conflict of interest arises that can be cured by the existence of a safeguard, the existence of the affiliation between an Applicant organization or Participant organization and audit personnel will be disclosed to the Joint Oversight Panel. The communication will include the safeguards explanation and how these safeguards do not compromise the ability to render a fair decision to the Applicant organization or Participant organization. Such affiliations include, but are not limited to, the following:
    13.1. Officers of the Applicant organization or Participant organization serving on the Accountability Agent's board of directors/board of managers in a voting capacity, and vice versa;
    13.2. Significant monetary arrangements or commercial relationship between the Accountability Agent and the Applicant organization or Participant organization, outside of the fee charged for certification and participation in the CBPR System; or
    13.3. All other affiliations which might allow the Applicant organization or Participant organization to exert undue influence on the Accountability Agent regarding the Applicant organization's certification and participation in the CBPR System.
14. Schellman will process all applications in the order received (i.e., preferential treatment is not provided to current clients, of any Schellman service) and schedule the certification assessment based on Schellman and the Client's availability.

See Appendix A: Conflicts of Interest

Program Requirements

15. Schellman utilized the assessment criteria outlined in the template documentation developed by APEC to map the CBPR Certification Program Requirements. Please see the attached Appendix B for the APEC assessment criteria mapped to Schellman's CBPR Program Requirements.

See Appendix B: CBPR Framework Requirements

Certification Process

Client Assessment

16. During the initial assessment of a new client or a reassessment of an existing client, Schellman will perform a formal review to help ensure that engaging the client does

not create a conflict of interest. The following requirements are considered during the assessment phase:

16.1. Certification shall not be considered or provided when a relationship poses an unacceptable threat to impartiality, such as a wholly owned subsidiary of Schellman requesting certification from its parent, and

16.2. Certification shall not be considered or provided for another Accountability Agent.

Scope and Planning

17. Based on information received from the organization, Schellman will determine the timing of the audit, assign the audit team members, and communicate to the organization the certification process, subsequent audits required to maintain certification, the dispute process, and any standard business terms applicable.

18. Upon agreement of the audit scope and timing between the client and Schellman, a job arrangement letter (JAL) or master services agreement (MSA) along with a statement of work (SOW) will be documented to address the contractual agreements between the client and Schellman pertaining to the certification services. Upon execution of the JAL or MSA/SOW, Schellman will provide the client with preliminary planning documents, which include, but are not limited to, the following:

18.1. Project Calendar outlining the testing areas to be performed by audit team members during the dates of fieldwork and dates and deadlines subsequent to the on-site assessment;

18.2. Information Request List (IRL) that documents each piece of evidence that the audit will need to determine compliance with the framework; and

18.3. The CBPR System Intake Questionnaire.

See Appendix C: CBPR System Intake Questionnaire

Fieldwork Process

The fieldwork process may include onsite time as well as remote fieldwork. The process includes the following activities:

19. Information gathering and analysis

19.1. Schellman will review the completed Intake Questionnaire provided by the client. Schellman will draft an IRL outlining the documentation to be provided by the client based on the responses from the completed Intake Questionnaire.

19.2. Schellman will review the documents provided by the client in response to the IRL provided to the client following the assessment criteria outlined within the Framework Requirements. Schellman will perform one or more testing

procedures that includes inquiry, observation and inspection of documentation. The below table defines these testing procedures:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related requirement. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, policies, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing may involve tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling Guidelines

20. Schellman has established a standard sampling methodology. Non-statistical samples are used and each client environment is evaluated to determine the impact of multi-site locations on the population and suggested sample sizes.

21. For any clients with multi-site locations, the audit team must determine the sample sizes required by location. Explanations must be documented in the client project files for any deviations from the standard sampling guidelines.

See Appendix F

Identification of Non-Compliant Requirements

22. The audit team is responsible for communicating inconsistencies and requirements that are not compliant to appropriate client personnel in a timely manner. Information related to the non-compliant requirements must be included within internal memorandums and supporting audit documentation.

23. Upon notification of non-compliant requirements, the client must analyze, document, and take corrective actions to remedy the identified issues within the timeframe provided by Schellman. Details regarding the corrective actions must be submitted to Schellman for review. The audit team will review the corrective actions and perform subsequent or additional testing as applicable. The minimum program requirements must be compliant prior to granting certification.

Report Deliverables

24. Schellman will issue a written audit report upon completion of the fieldwork to the Applicant organization noting the organization's level of compliance with the program requirements. Where non-fulfillment or non-compliance of any of the program requirements is found, the report must include a list of changes the Applicant organization needs to complete for purposes of obtaining certification for participation in the CBPR System as well as the required timeframe for completion. The report will also outline the corrective actions, if those were communicated to Schellman by the Applicant organization.

25. If all requirements are compliant, the audit report will confirm compliance with the program requirements.

Certification Seal Policy

26. The Schellman certification seal is a service mark of Schellman. The Schellman certification seal may not be used in connection with any product or service that was not within the scope of the CBPR certification review, or in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Schellman. The certification seal should be used only upon the granting or extending of a CBPR certification.

27. Schellman provides public access to information about its certification process on the Schellman website (https://www.schellman.com/apec/cbpr-process#requirements). Information about the certification status that includes the granting, extending, maintaining, enforcing, renewing, suspending, reducing the scope of, or withdrawing of certification of any organization will be publicly provided through the website.

28. Schellman maintains a directory of valid certifications (https://www.schellman.com/apec-certificate-directory) that at a minimum show the name of the certified organization, a website for the certified organization and a link to the organization's privacy notice, contact information, the scope of the certification, the organization's original certification date, and the date that the current certification expires.

Ongoing Monitoring and Compliance Review Process

29. Participants are monitored throughout the certification period to ensure compliance with the program. The monitoring process may include periodic reviews of the Participant's privacy notice for updates or modifications. It may also include a review of any matters disclosed on the Participant's website, other than the privacy notice. Where changes or modifications occur that are not compliant with the program requirements, or result in significant changes, the recertification process will be immediately implemented as described below, which may include short-notice or unannounced audits.

30. Where there are reasonable grounds to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements, an immediate review process will be triggered whereby verification of compliance will be carried out. In these situations, the Dispute process, as outlined below, will be followed.

31. The dispute process provides another method of on-going monitoring and compliance review during the certification period. Where non-compliance with any of the program requirements is found, Schellman will notify the Participant as outlined in the Dispute process outlined below. As the Dispute process outlines, Schellman will verify that the required changes have been properly completed by the Participant within the stated timeframe. At such time, the certification will be suspended until Schellman can verify that the Participant is in compliance with the requirements.

Recertification and Annual Attestation

32. In order for Participants to maintain their certification, recertification must take place at least every year following the date of initial certification.

33. There are occasions when Schellman must conduct audits of certified clients at short notice or unannounced to investigate complaints, or in response to changes, or as follow-up on suspended clients.

34. When Schellman determines that an unannounced or short-notice audit is required, Schellman describes and makes known in advance to the certified client the conditions under which these short-notice visits are to be conducted.

35. Prior to recertification, Schellman will determine adjustments to audit time and resources based on modifications to the client scope. Client personnel are required to disclose significant changes within their organization to Schellman.

36. The recertification process will include:

    36.1. An updated and completed CBPR Intake Questionnaire provided by the client. Schellman will review the completed form looking for any changes since the initial certification.

    36.2. Regardless of whether any changes have occurred, Schellman will perform the recertification in the same manner as the initial certification assessment, as outlined above.

    36.3. An audit report will be provided to the Participant outlining the Accountability Agent's findings regarding the Participant's level of compliance with the program requirements. The report will include any areas of non-compliance and corrections the Participant needs to make to correct areas and the

timeframe within which the corrections must be completed for purposes of obtaining recertification.

36.4. If non-compliance areas were found during the recertification process, Schellman will review documentation provided by the Participant to verify that correction has been completed and is compliant, prior to obtaining recertification.

36.5. Upon verification that the requirements are in compliance, a final report will be provided to the Participant as notice of compliance with the program requirements and that the Participant has been recertified.

Dispute Resolution Process

37. Schellman utilizes its current dispute process to receive, investigate and resolve complaints about Participants. The dispute process is handled by Schellman and is not outsourced. Additionally, the dispute process is available via the Schellman website and is outlined below.

Receiving Disputes and Consent

38. Any dispute, or complaint, is required to be formally submitted using the form at https://www.schellman.com/apec/stats. The complaint should include the reason for complaint, the date of the complaint, and any evidence supporting the complaint. The form will include a consent to share any personal information with any third parties, including the relevant enforcement authority, in connection with a request for assistance. Submission, investigation, and decision on complaints do not result in any discriminatory actions against the complainant.

39. Each complaint is logged and recorded including the date the complaint was received and by whom it was received.

40. Each complaint will be investigated to determine whether it concerns the Participant's obligations under the program and if the complaint falls within the scope of the certification and requirements.

Dispute Notification

41. Once the complaint is received, the individual that submitted the complaint will be notified to confirm the complaint and the determination made based on the review outlined above. A confirmation of receipt of the complaint is required to be provided to the individual submitting the complaint within five business days.

Investigating Disputes

42. Investigation of disputes might include cooperation with other Accountability Agents, as recognized by the APEC economies.

43. The time necessary to resolve a complaint may vary due to the extent of the complaint, any required due diligence, and the formality of the response. A progress update is to be provided to the individual submitting the complaint at a minimum once per month.

Resolving Disputes

44. If noncompliance was found with any of the program requirements, Schellman will contact the Participant outlining the details of the noncompliance that require remediation and the required timeframe for completion. At such time, the certificate will be suspended.

45. The Participant is required to provide evidence of remediation within the required timeframe for the certification to be reinstated. If the Participant fails to provide sufficient evidence, during the required timeframe, or is not responsive, the certification will remain suspended. The timeframe shall not exceed a period of six (6) months or upon the due date of the annual recertification.

46. If Schellman receives sufficient evidence of the remediation within the required timeframe, the suspension will be removed and the certificate will be reinstated.

47. Schellman will provide written notice of complaint resolution to the complainant and the Participant.

Publicly Available Statistics and Case Notes

48. Schellman will include statistics on the types of complaints received by Schellman and the outcomes of such complaints on the company website, that is publicly available. This information will be provided to the FTC and the Joint Oversight Panel during recertification or as required to be reported.

See Appendix E: Complaint Statistics Template

49. Schellman will maintain, and release in an anonymized form during recertification or as required, case notes on a selection of resolved complaints, illustrating typical or significant interpretations and notable outcomes.

See Appendix D: Case Notes Template

Mechanism for Enforcing Program Requirements

50. Schellman has the authority to enforce its program requirements against clients, or Participants, through the JAL or MSA/SOW. Schellman has the authority to suspend, withdraw, or reduce the scope of a certification under just cause and as a result of reasonable evidence.

51. Certification shall be suspended in cases when, for example:
    51.1. The client was found to be in noncompliance within the scope of the program's requirements throughout the certification period, including identification during the initial certification; recertification; ongoing monitoring; or the dispute process, and the findings have not been resolved within the required timeframes, which shall not exceed a period of six (6) months or upon the due date of the annual recertification;
    51.2. The certified client does not allow recertification audits to be conducted at the required frequencies;
    51.3. Where there are reasonable grounds to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements; or
    51.4. The certified client has voluntarily requested a suspension.

52. As previously noted, if noncompliance was found with any of the program requirements, Schellman will contact the Participant outlining the details of the noncompliance that require remediation and the required timeframe for completion.

53. The certificate is suspended until the Participant has provided sufficient evidence of the remediation within the required timeframe, which shall not exceed a period of six (6) months or upon the due date of the annual recertification. Upon receipt of sufficient evidence of remediation within the required timeframe, Schellman will perform a review of the evidence to determine if the certificate should be reinstated. The results are communicated to the client via an audit report. Failure to resolve the issues that have resulted in the suspension in the time established by Schellman will result in withdrawal or reduction of the scope of certification, if applicable.

    A reduction in the scope of the certification may be applicable and would exclude the parts not meeting the requirements, when the client has persistently or seriously failed to meet the program requirements for those parts of the scope of certification.

54. Under suspension, the client's certification is temporarily invalid. Included within the JAL or MSA/SOW are the enforceable arrangements regarding the suspension of the certification to help ensure, that in case of suspension, the client refrains from further promotion of its certification and use of the Schellman certification seal. Schellman will make publicly accessible, on the company website, the suspended status of the certification.

55. Schellman is required to refer the violation to the Federal Trade Commission, where a reasonable belief is pursuant to its established review process that a client's failure to comply with the APEC CBPR System has not been remedied within a reasonable time, so long as such failure to comply can be reasonably believed to be a violation of applicable law. Schellman will respond to requests from enforcement entities in

APEC Economies that reasonably relate to that Economy and to the CBPR related activities of Schellman.

56. If the determination is to withdrawal the certification, Schellman, as included in the JAL or MSA/SOW, has enforceable arrangements with the Participant concerning conditions of withdrawal, ensuring upon notice of withdrawal of certification that the client discontinues its use of all advertising matter that contains any reference to a certified status.

57. Upon request by any party, Schellman will correctly state the status of certification of the participant, or client, as being suspended, withdrawn, or reduced.

CBPR Framework: Appendices

Appendix A: Conflicts of Interest Policy

CONFLICTS OF INTEREST

All employees have a duty to further the Company's aims and goals, and to work on behalf of its best interest. Employees should not place themselves in a position where the employee's actions or personal interests may be in conflict with those of the Company.

Examples include, but are not limited to, the following:

- Self-interest threats: threats that arise from a person or body acting in their own interest. A concern related to certification, as a threat to impartiality, is financial self-interest.
- Self-review threats: threats that arise from a person or body reviewing the work done by themselves. Auditing the program requirements of an Applicant organization or Participant organization to whom Schellman provided consultancy would be a self-review threat.
- Familiarity (or trust) threats: threats that arise from a person or body being too familiar with or trusting of another person instead of seeking audit evidence.
- Intimidation threats: threats that arise from a person or body having a perception of being coerced openly or secretively, such as a threat to be replaced or reported to a supervisor.
- Officers of the Applicant organization or Participant organization serving on the Accountability Agent's board of directors in a voting capacity, and vice versa.
- Significant monetary arrangements or commercial relationship between the Accountability Agent and the Applicant organization or Participant organization, outside of the fee charged for certification and participation in the APEC CBPR or PRP System.
- All other affiliations which might allow the Applicant organization or Participant organization to exert undue influence on the Accountability Agent regarding the Applicant organization's certification and participation in the CBPR or PRP System.

Employees should report to their manager any situation or position (including outside employment by the employee or any member of the employee's immediate household) which may create a conflict of interest with the Company. Additionally, employees are required to complete an annual independence review and disclose any potential conflict of interest. Human resources and management review the results from the annual independence review. Having relationships does not necessarily present the Company with a conflict of interest; however, if any relationship creates a threat to impartiality, the Company is required to document and be able to demonstrate how it eliminates or minimizes such threats. Threats identified as a result of the Independence Review that could impact the impartiality of the services provided by Schellman will be handled on a per-incident basis and where appropriate, Schellman will withdraw from the engagement. If a conflict of interest arises that can be cured by the existence of a safeguard, the existence of the affiliation between an Applicant organization or Participant organization and audit personnel will be disclosed to the Joint Oversight Panel. The communication will include the safeguards explanation and how these safeguards do not compromise the ability to render a fair decision to the Applicant organization or Participant organization.

Schellman is solely responsible for the decisions for granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing certification. Schellman does not outsource any activities related to the certification services that it provides. Schellman also does not offer or provide consulting or technical services to any client includes those services related to the development or implementation of Participant organization's or Applicant organization's data privacy practices and procedures. Schellman does not perform internal audits for any client. Personnel handling sales for Schellman that may collect a sales commission will not be part of the certification audit team for an Applicant organization or Participant organization.

Appendix B: CBPR Framework Requirements

NOTICE

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

Please note the additional column to the far right for mapping of Schellman's Certification Requirements to these APEC CBPR Framework Requirements. The yellow highlight serves to provide easy reference to the mapped areas.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline. • States an effective date of Privacy Statement publication. Where Applicant answers **NO to question 1** and does not identify an applicable qualification subject to the Qualifications to Notice set out **below**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*Notice* 1. The privacy notice or statement must provide clear and easily accessible statements about your practices and policies that govern personal information and must include the following: a. Outline the services covered by the notice or statement; b. Be available on the client's Website, such as text on a Web page, link from URL, attached document, pop-up windows, or included in frequently asked questions (FAQs); c. Be easy to find and be accessible; d. Include an effective date; e. Name of the organization and location; f. Include information on how to contact the organization about the practices and handling of personal information upon collection; g. Apply to all personal information, whether collected online or offline; *Accountability* 1. Implement measures to ensure compliance the APEC Information Privacy Principles.
1.a) Does this privacy statement describe how	If **YES**, the Accountability Agent must verify that:	*Notice*

Question	Assessment Criteria	Schellman Minimum Certification Requirement
personal information is collected?	• The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. • the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	1. The privacy notice or statement must provide clear and easily accessible statements about your practices and policies that govern personal information and must include the following: a. Outline the services covered by the notice or statement; b. Be available on the client's Website, such as text on a Web page, link from URL, attached document, pop-up windows, or included in frequently asked questions (FAQs); c. Be easy to find and be accessible; d. Include an effective date; e. Name of the organization and location; f. Include information on how to contact the organization about the practices and handling of personal information upon collection; g. Apply to all personal information, whether collected online or offline; h. Describe the collection practices and policies applied to all covered personal information collected by the client (i.e., how your organization collects personal information); i. Indicate what types of personal information, whether collected directly or through a third party or agent, are collected; j. Report the categories or specific sources of all categories of personal information collected;
1.b) Does this privacy statement describe the purpose(s) for which	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals	*Notice* 1. The privacy notice or statement must provide clear and easily accessible statements about your

Question	Assessment Criteria	Schellman Minimum Certification Requirement
personal information is collected?	of the purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	practices and policies that govern personal information and must include the following: a. Outline the services covered by the notice or statement; b. Be available on the client's Website, such as text on a Web page, link from URL, attached document, pop-up windows, or included in frequently asked questions (FAQs); c. Be easy to find and be accessible; d. Include an effective date; e. Name of the organization and location; f. Include information on how to contact the organization about the practices and handling of personal information upon collection; g. Apply to all personal information, whether collected online or offline; h. Describe the collection practices and policies applied to all covered personal information collected by the client (i.e., how your organization collects personal information); i. Indicate what types of personal information, whether collected directly or through a third party or agent, are collected; j. Report the categories or specific sources of all categories of personal information collected; k. Describe the purpose(s) for which personal information is collected;
1.c) Does this privacy statement inform individuals whether their	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third	*Notice* 1. The privacy notice or statement must provide clear and easily accessible statements about your

Question	Assessment Criteria	Schellman Minimum Certification Requirement
personal information is made available to third parties and for what purpose?	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 answers **NO** and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	practices and policies that govern personal information and must include the following: a. Outline the services covered by the notice or statement; b. Be available on the client's Website, such as text on a Web page, link from URL, attached document, pop-up windows, or included in frequently asked questions (FAQs); c. Be easy to find and be accessible; d. Include an effective date; e. Name of the organization and location; f. Include information on how to contact the organization about the practices and handling of personal information upon collection; g. Apply to all personal information, whether collected online or offline; h. Describe the collection practices and policies applied to all covered personal information collected by the client (i.e., how your organization collects personal information); i. Indicate what types of personal information, whether collected directly or through a third party or agent, are collected; j. Report the categories or specific sources of all categories of personal information collected; k. Describe the purpose(s) for which personal information is collected; l. Inform individuals as to whether information is shared with third parties and for what purpose you make personal information available to third parties including the

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		identification of **the categories or specific third parties**;
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a **functional** e-mail address. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*Notice* 1. The privacy notice or statement must provide clear and easily accessible statements about your practices and policies that govern personal information and must include the following: a. Outline the services covered by the notice or statement; b. Be available on the client's Website, such as text on a Web page, link from URL, attached document, pop-up windows, or included in frequently asked questions (FAQs); c. Be easy to find and be accessible; d. Include an effective date; e. Name of the organization and location; f. Include information on how to contact the organization about the practices and handling of personal information upon collection;
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*Notice* 1. The privacy notice or statement must provide clear and easily accessible statements about your practices and policies that govern personal information and must include the following: a. Outline the services covered by the notice or statement; b. Be available on the client's Website, such as text on a Web page, link from URL, attached document, pop-up windows, or included in frequently asked questions (FAQs); c. Be easy to find and be accessible;

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		d. Include an effective date; e. Name of the organization and location; f. Include information on how to contact the organization about the practices and handling of personal information upon collection; g. Apply to all personal information, whether collected online or offline; h. Describe the collection practices and policies applied to all covered personal information collected by the client (i.e., how your organization collects personal information); i. Indicate what types of personal information, whether collected directly or through a third party or agent, are collected; j. Report the categories or specific sources of all categories of personal information collected; k. Describe the purpose(s) for which personal information is collected; l. Inform individuals as to whether information is shared with third parties and for what purpose you make personal information available to third parties including the identification of **the categories or specific third parties**; m. Include information regarding the use and disclosure of an individual's personal information;
1.f) Does this privacy statement provide information regarding whether and how an individual can access and	Where the Applicant answers **YES**, the Accountability Agent must verify that the Privacy Statement includes:	*Notice* 1. The privacy notice or statement must provide clear and easily accessible statements about your practices and policies that govern personal information and must include the following:

Question	Assessment Criteria	Schellman Minimum Certification Requirement
correct their personal information?	• The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). • The process that an individual must follow in order to correct his or her personal information Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	a. Outline the services covered by the notice or statement; b. Be available on the client's Website, such as text on a Web page, link from URL, attached document, pop-up windows, or included in frequently asked questions (FAQs); c. Be easy to find and be accessible; d. Include an effective date; e. Name of the organization and location; f. Include information on how to contact the organization about the practices and handling of personal information upon collection; g. Apply to all personal information, whether collected online or offline; h. Describe the collection practices and policies applied to all covered personal information collected by the client (i.e., how your organization collects personal information); i. Indicate what types of personal information, whether collected directly or through a third party or agent, are collected; j. Report the categories or specific sources of all categories of personal information collected; k. Describe the purpose(s) for which personal information is collected; l. Inform individuals as to whether information is shared with third parties and for what purpose you make personal information available to third parties including the

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		identification of **the categories or specific third parties**; m. Include information regarding the use and disclosure of an individual's personal information; n. Include information regarding whether and how an individual can access and correct their personal information including the following: i. The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means); ii. The process that an individual must follow in order to correct his or her personal information;
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 answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected **and that the notice is reasonably available to individuals**. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*Notice* 1. The privacy notice or statement must provide clear and easily accessible statements about your practices and policies that govern personal information and must include the following: a. Outline the services covered by the notice or statement; b. Be available on the client's Website, such as text on a Web page, link from URL, attached document, pop-up windows, or included in frequently asked questions (FAQs); c. Be easy to find and be accessible; d. Include an effective date; e. Name of the organization and location; f. Include information on how to contact the organization about the practices and

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		handling of personal information upon collection; g. Apply to all personal information, whether collected online or offline; h. Describe the collection practices and policies applied to all covered personal information collected by the client (i.e., how your organization collects personal information); i. Indicate what types of personal information, whether collected directly or through a third party or agent, are collected; j. Report the categories or specific sources of all categories of personal information collected; k. Describe the purpose(s) for which personal information is collected; l. Inform individuals as to whether information is shared with third parties and for what purpose you make personal information available to third parties including the identification of **the categories or specific third parties**; m. Include information regarding the use and disclosure of an individual's personal information; n. Include information regarding whether and how an individual can access and correct their personal information including the following: i. The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means);

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		ii. The process that an individual must follow in order to correct his or her personal information; o. Provide notice to the individual at the time of collection of personal information, whether directly or through the use of third parties acting on your behalf, that such information is being collected*; * The following are situations in which the application at the time of collection of the APEC Notice Principle may not be necessary or practical. Justification for any of the following will be required. **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). **Collection of Publicly Available Information**: Personal information controllers do not need to provide notice regarding the collection and use of publicly available information. **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. **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. **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.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		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. **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. **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.
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*Notice* 1. The privacy notice or statement must provide clear and easily accessible statements about your practices and policies that govern personal information and must include the following: a. Outline the services covered by the notice or statement; b. Be available on the client's Website, such as text on a Web page, link from URL, attached document, pop-up windows, or included in frequently asked questions (FAQs); c. Be easy to find and be accessible; d. Include an effective date; e. Name of the organization and location; f. Include information on how to contact the organization about the practices and handling of personal information upon collection; g. Apply to all personal information, whether collected online or offline; h. Describe the collection practices and policies applied to all covered personal information collected by the client (i.e., how

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		your organization collects personal information); i. Indicate what types of personal information, whether collected directly or through a third party or agent, are collected; j. Report the categories or specific sources of all categories of personal information collected; k. Describe the purpose(s) for which personal information is collected; l. Inform individuals as to whether information is shared with third parties and for what purpose you make personal information available to third parties including the identification of **the categories or specific third parties**; m. Include information regarding the use and disclosure of an individual's personal information; n. Include information regarding whether and how an individual can access and correct their personal information including the following: i. The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means); ii. The process that an individual must follow in order to correct his or her personal information; o. Provide notice to the individual at the time of collection of personal information, whether directly or through the use of third

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		parties acting on your behalf, that such information is being collected*; p. Indicate the purpose(s) for which personal information is being collected at the time of collection of personal information, whether directly or through the use of third parties acting on your behalf*(the communication must be in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other); * The following are situations in which the application at the time of collection of the APEC Notice Principle may not be necessary or practical. Justification for any of the following will be required. **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). **Collection of Publicly Available Information**: Personal information controllers do not need to provide notice regarding the collection and use of publicly available information. **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. **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. **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

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		form of process such as a discovery request made in the course of civil litigation. **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. **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. **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.
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 answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.	*Notice* 1. The privacy notice or statement must provide clear and easily accessible statements about your practices and policies that govern personal information and must include the following: a. Outline the services covered by the notice or statement; b. Be available on the client's Website, such as text on a Web page, link from URL, attached document, pop-up windows, or included in frequently asked questions (FAQs); c. Be easy to find and be accessible; d. Include an effective date; e. Name of the organization and location; f. Include information on how to contact the organization about the practices and handling of personal information upon collection; g. Apply to all personal information, whether collected online or offline;

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		h. Describe the collection practices and policies applied to all covered personal information collected by the client (i.e., how your organization collects personal information); i. Indicate what types of personal information, whether collected directly or through a third party or agent, are collected; j. Report the categories or specific sources of all categories of personal information collected; k. Describe the purpose(s) for which personal information is collected; l. Inform individuals as to whether information is shared with third parties and for what purpose you make personal information available to third parties including the identification of **the categories or specific third parties**; m. Include information regarding the use and disclosure of an individual's personal information; n. Include information regarding whether and how an individual can access and correct their personal information including the following: i. The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means); ii. The process that an individual must follow in order to correct his or her personal information;

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		o. Provide notice to the individual at the time of collection of personal information, whether directly or through the use of third parties acting on your behalf, that such information is being collected*; p. Indicate the purpose(s) for which personal information is being collected at the time of collection of personal information, whether directly or through the use of third parties acting on your behalf*(the communication must be in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other); q. Provide notice to the individual at the time of collection of personal information, that their personal information may be shared with third parties.* * The following are situations in which the application at the time of collection of the APEC Notice Principle may not be necessary or practical. Justification for any of the following will be required. **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). **Collection of Publicly Available Information**: Personal information controllers do not need to provide notice regarding the collection and use of publicly available information. **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.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		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. **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. **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. **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. **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	Schellman Minimum Certification Requirement
5. How do you obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf? 5.c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES to any of these sub-parts**, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	*Collection* 1. The collection of personal information must be limited to information that is relevant to the purposes of collection, consistent with the requirements of the jurisdiction where data was collected, and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned. 2. Identify the type of data collected, the economies where data is collected, the source (i.e., the individual or a third party) and the corresponding purposes and use of collection for each type of data.
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 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 to identify: • Each type of data collected • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data • An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes	*Collection* 1. The collection of personal information must be limited to information that is relevant to the purposes of collection, consistent with the requirements of the jurisdiction where data was collected, and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
	Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	*Collection* 1. The collection of personal information must be limited to information that is relevant to the purposes of collection, consistent with the requirements of the jurisdiction where data was collected, and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

USES OF PERSONAL INFORMATION

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

Question	Assessment Criteria	Schellman Minimum Certification Requirement
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	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes.	*Use* *1.* Personal information collected must be used only to fulfill the purposes of collection and other compatible or related purposes as identified in the privacy statement and/or in the notice provided at the time of collection except for one of the following: *a.* With the consent of the individual whose personal information is collected;

Question	Assessment Criteria	Schellman Minimum Certification Requirement
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 Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	i. Consent must be a documented description or documentation that consent was obtained *b.* When necessary to provide a service or product requested by the individual; or *i.* A description must be documented of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual *c.* By the authority of law and other legal instruments, proclamations and pronouncements of legal effect. *i.* A description must be documented of how collected information shared, used or disclosed as compelled by law including the legal requirements under which it is compelled to share the personal information, unless the client is bound by confidentiality requirements For the purposes of this Principle, uses of personal information include the transfer or disclosure of personal information.
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual?	Where the Applicant answers **NO** to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as: • Online at point of collection	*Use* *1.* Personal information collected must be used only to fulfill the purposes of collection and other compatible or related purposes as identified in the privacy statement and/or in the notice provided at the time of collection except for one of the following: *a.* With the consent of the individual whose personal information is collected; i. Consent must be a documented description or documentation that consent was obtained

Question	Assessment Criteria	Schellman Minimum Certification Requirement
9.b) Compelled by applicable laws?	• Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	*b.* When necessary to provide a service or product requested by the individual; or *i.* A description must be documented of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual *c.* By the authority of law and other legal instruments, proclamations and pronouncements of legal effect. *i.* A description must be documented of how collected information shared, used or disclosed as compelled by law including the legal requirements under which it is compelled to share the personal information, unless the client is bound by confidentiality requirements For the purposes of this Principle, uses of personal information include the transfer or disclosure of personal information.
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. 11. Do you transfer personal information to personal information processors? If YES, describe.	Where the Applicant 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 to identify: 1) each type of data disclosed or transferred;	2. 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. The organization must: *a.* Identify the type of data disclosed or transferred, the economies where data was transferred, the corresponding purpose of collection for each type of disclosed data, and

Question	Assessment Criteria	Schellman Minimum Certification Requirement
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.	2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.).
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the individual? 13.c) Compelled by applicable laws?	Where applicant answers **NO** to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers **YES** to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers **YES** to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual.	*Use* *1.* Personal information collected must be used only to fulfill the purposes of collection and other compatible or related purposes as identified in the privacy statement and/or in the notice provided at the time of collection except for one of the following: *a.* With the consent of the individual whose personal information is collected; i. Consent must be a documented description or documentation that consent was obtained *b.* When necessary to provide a service or product requested by the individual; or *i.* A description must be documented of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual *c.* By the authority of law and other legal instruments, proclamations and pronouncements of legal effect. *i.* A description must be documented of how collected information shared, used or disclosed as compelled by law including the legal requirements under which it is

Question	Assessment Criteria	Schellman Minimum Certification Requirement
	Where the Applicant answers **YES** to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	compelled to share the personal information, unless the client is bound by confidentiality requirements For the purposes of this Principle, uses of personal information include the transfer or disclosure of personal information.

CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organizations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.*

Question	Assessment Criteria	Schellman Minimum Certification Requirement
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	*Choice* 1. A mechanism* must be provided for individuals to exercise choice in relation to the collection of their personal information. *The following are situations in which the application of the APEC Choice Principle may not be necessary or practical. Justification for any of the following will be required. **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. **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. **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. **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. **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

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		purposes where the provision of such mechanism to the individual will likely prejudice the investigation. **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. **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. **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.
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 answers **YES**, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity	*Choice* 1. A mechanism* must be provided for individuals to exercise choice in relation to the collection of their personal information. 2. A mechanism* must be provided for individuals to exercise choice in relation to the use of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. 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 b. Personal information may be disclosed or distributed to third parties, other than Service Providers.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
	to exercise choice may be provided to the individual after collection, but before:] • being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	*The following are situations in which the application of the APEC Choice Principle may not be necessary or practical. Justification for any of the following will be required. **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. **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. **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. **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. **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. **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. **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

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		of a violation of a code of conduct, breach of contract or a contravention of domestic law. **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.
16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected.] Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice	*Choice* 1. A mechanism* must be provided for individuals to exercise choice in relation to the collection of their personal information. 2. A mechanism* must be provided for individuals to exercise choice in relation to the use of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. 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 b. Personal information may be disclosed or distributed to third parties, other than Service Providers. 3. A mechanism* must be provided for individuals to exercise choice in relation to the disclosure of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. Disclosing the personal information to third parties, other than Service Providers.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
	and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	*The following are situations in which the application of the APEC Choice Principle may not be necessary or practical. Justification for any of the following will be required. **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. **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. **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. **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. **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. **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. **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

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		of a violation of a code of conduct, breach of contract or a contravention of domestic law. **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.
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	*Choice* 1. A mechanism* must be provided for individuals to exercise choice in relation to the collection of their personal information. 2. A mechanism* must be provided for individuals to exercise choice in relation to the use of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. 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 b. Personal information may be disclosed or distributed to third parties, other than Service Providers. 3. A mechanism* must be provided for individuals to exercise choice in relation to the disclosure of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. Disclosing personal information to third parties, other than Service Providers.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		4. Choices must be displayed or provided in a clear and conspicuous manner, clearly worded and easily understandable, and easily accessible and affordable.
18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers **NO**, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	*Choice* 1. A mechanism* must be provided for individuals to exercise choice in relation to the collection of their personal information. 2. A mechanism* must be provided for individuals to exercise choice in relation to the use of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. 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 b. Personal information may be disclosed or distributed to third parties, other than Service Providers. 3. A mechanism* must be provided for individuals to exercise choice in relation to the disclosure of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. Disclosing personal information to third parties, other than Service Providers. 4. Choices must be displayed or provided in a clear and conspicuous manner, clearly worded and easily

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		understandable, and easily accessible and affordable.
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 and affordable? Where YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	*Choice* 1. A mechanism* must be provided for individuals to exercise choice in relation to the collection of their personal information. 2. A mechanism* must be provided for individuals to exercise choice in relation to the use of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. 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 b. Personal information may be disclosed or distributed to third parties, other than Service Providers. 3. A mechanism* must be provided for individuals to exercise choice in relation to the disclosure of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. Disclosing the personal information to third parties, other than Service Providers. Choices must be displayed or provided in a clear and conspicuous manner, clearly worded and easily understandable, and easily accessible and affordable.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	*Choice* 1. A mechanism* must be provided for individuals to exercise choice in relation to the collection of their personal information. 2. A mechanism* must be provided for individuals to exercise choice in relation to the use of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. 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 b. Personal information may be disclosed or distributed to third parties, other than Service Providers. 3. A mechanism* must be provided for individuals to exercise choice in relation to the disclosure of their personal information. 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. The opportunity to exercise choice may be provided to the individual after collection, but before: a. Disclosing personal information to third parties, other than Service Providers. 4. Choices must be displayed or provided in a clear and conspicuous manner, clearly worded and easily understandable, and easily accessible and affordable. *The following are situations in which the application of the APEC Choice Principle may not be necessary or practical. Justification for any of the following will be required.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		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. **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. **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. **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. **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. **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. **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.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		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 Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use*

Question	Assessment Criteria	Schellman Minimum Certification Requirement
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. **The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use**. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	*Integrity of Personal Information* 1. Personal information must be accurate, complete and kept up-to date to the extent necessary for the purposes of use.
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 answers **YES**, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and 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 answers **NO**, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the	*Integrity of Personal Information* 1. Personal information must be accurate, complete and kept up-to date to the extent necessary for the purposes of use. 2. Provide individuals the ability to challenge the accuracy of their personal information and to have it rectified, completed, amended and/or deleted and ensure procedures are in place to complete the request including communication and confirmation of the request to processors, agent, or other service providers to whom the personal information was transferred. Access and correction mechanisms must be presented in a clear and conspicuous manner. The request should be completed within a reasonable time frame following the request and

Question	Assessment Criteria	Schellman Minimum Certification Requirement
	purposes of use, are required for compliance with this principle.	confirmation should be provided that the request has been completed.
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	*Integrity of Personal Information* 1. Personal information must be accurate, complete and kept up-to date to the extent necessary for the purposes of use. 2. Provide individuals the ability to challenge the accuracy of their personal information and to have it rectified, completed, amended and/or deleted and ensure procedures are in place to complete the request including communication and confirmation of the request to processors, agent, or other service providers to whom the personal information was transferred. Access and correction mechanisms must be presented in a clear and conspicuous manner. The request should be completed within a reasonable time frame following the request and a confirmation should be provided that the request has been completed.
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 answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant 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 answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	*Integrity of Personal Information* 1. Personal information must be accurate, complete and kept up-to date to the extent necessary for the purposes of use. 2. Provide individuals the ability to challenge the accuracy of their personal information and to have it rectified, completed, amended and/or deleted and ensure procedures are in place to complete the request including communication and confirmation of the request to processors, agent, or other service providers to whom the personal information was transferred. Access and correction mechanisms must be presented in a clear and conspicuous manner. The request should be completed within a reasonable time frame following the request and a

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		confirmation should be provided that the request has been completed.
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	*Integrity of Personal Information* 1. Personal information must be accurate, complete and kept up-to date to the extent necessary for the purposes of use. 2. Provide individuals the ability to challenge the accuracy of their personal information and to have it rectified, completed, amended and/or deleted and ensure procedures are in place to complete the request including communication and confirmation of the request to processors, agent, or other service providers to whom the personal information was transferred. Access and correction mechanisms must be presented in a clear and conspicuous manner. The request should be completed within a reasonable time frame following the request and confirmation should be provided that the request has been completed. 3. If correction is denied, an explanation should be provided, together with contact information for further inquiries about the denial of access or correction 4. Require 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 and ensure procedures are in place to complete the correction.

SECURITY SAFEGUARDS

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

Question	Assessment Criteria	Schellman Minimum Certification Requirement
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	*Security Safeguards* 1. Maintain a written information security policy.
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • **Authentication and access control (eg password protections)** • **Encryption** • **Boundary protection (eg firewalls, intrusion detection)** • **Audit logging** • **Monitoring (eg external and internal audits, vulnerability scans)** • **Other (specify)** The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.	*Security Safeguards* 1. Maintain a written information security policy. 2. Implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. 3. Communicate to employees their obligations and the importance of maintaining the security of personal information. 4. Require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. Such requirement should include: a. Implementing an information security program that is proportionate to the sensitivity of the information and services provided

Question	Assessment Criteria	Schellman Minimum Certification Requirement
	Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	b. Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information c. Taking immediate steps to correct/address the security failure which caused the privacy or security breach
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 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 must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	*Security Safeguards* 1. Maintain a written information security policy. 2. Implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. 3. Communicate to employees their obligations and the importance of maintaining the security of personal information. 4. Require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction,

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		use, modification or disclosure or other misuses of the information. Such requirement should include: a. Implementing an information security program that is proportionate to the sensitivity of the information and services provided b. Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information c. Taking immediate steps to correct/address the security failure which caused the privacy or security breach
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, **and obligations respecting**, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	*Security Safeguards* 1. Maintain a written information security policy. 2. Implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. 3. Communicate to employees their obligations and the importance of maintaining the security of personal information.
30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable	*Security Safeguards* 1. Maintain a written information security policy. 2. Implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity

Question	Assessment Criteria	Schellman Minimum Certification Requirement
context in which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures? 30.d) Physical security?	means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.	of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. 3. Communicate to employees their obligations and the importance of maintaining the security of personal information. 4. Require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. Such requirement should include: a. Implementing an information security program that is proportionate to the sensitivity of the information and services provided b. Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information c. Taking immediate steps to correct/address the security failure which caused the privacy or security breach 5. Maintain a policy for secure disposal of personal information. 6. Implement procedures to detect, prevent, and respond to attacks, intrusions, or other security failures. 7. Perform tests on a periodic basis on the effectiveness of the implemented physical, technical and administrative safeguards. 8. Perform risk assessments or third-party validations on a periodic basis that include the implemented physical, technical and administrative safeguards and review the results of the assessment or third-party validation for remediation.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	*Security Safeguards* 1. Maintain a written information security policy. 2. Implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. 3. Communicate to employees their obligations and the importance of maintaining the security of personal information. 4. Require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. Such requirement should include: a. Implementing an information security program that is proportionate to the sensitivity of the information and services provided b. Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information c. Taking immediate steps to correct/address the security failure which caused the privacy or security breach 5. Maintain a policy for secure disposal of personal information.
32. Have you implemented measures to detect, prevent, and	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures.	*Security Safeguards* 1. Maintain a written information security policy. 2. Implement physical, technical and administrative safeguards to protect personal information against

Question	Assessment Criteria	Schellman Minimum Certification Requirement
respond to attacks, intrusions, or other security failures?	Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. 3. Communicate to employees their obligations and the importance of maintaining the security of personal information. 4. Require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. Such requirement should include: a. Implementing an information security program that is proportionate to the sensitivity of the information and services provided b. Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information c. Taking immediate steps to correct/address the security failure which caused the privacy or security breach 5. Maintain a policy for secure disposal of personal information. 6. Implement procedures to detect, prevent, and respond to attacks, intrusions, or other security failures.
33. Do you have processes in place to test the effectiveness of the safeguards referred to	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	*Security Safeguards* 1. Maintain a written information security policy. 2. Implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access,

Question	Assessment Criteria	Schellman Minimum Certification Requirement
above in question 32? Describe below.		destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. 3. Communicate to employees their obligations and the importance of maintaining the security of personal information. 4. Require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. Such requirement should include: a. Implementing an information security program that is proportionate to the sensitivity of the information and services provided b. Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information c. Taking immediate steps to correct/address the security failure which caused the privacy or security breach 5. Maintain a policy for secure disposal of personal information. 6. Implement procedures to detect, prevent, and respond to attacks, intrusions, or other security failures. 7. Perform tests on a periodic basis on the effectiveness of the implemented physical, technical and administrative safeguards.
34. Do you use **risk assessments or third-**	The Accountability Agent must verify that such **risk assessments or certifications** are undertaken at	*Security Safeguards* 1. Maintain a written information security policy.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
party certifications? Describe below.	appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	2. Implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. 3. Communicate to employees their obligations and the importance of maintaining the security of personal information. 4. Require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. Such requirement should include: a. Implementing an information security program that is proportionate to the sensitivity of the information and services provided b. Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information c. Taking immediate steps to correct/address the security failure which caused the privacy or security breach 5. Maintain a policy for secure disposal of personal information. 6. Implement procedures to detect, prevent, and respond to attacks, intrusions, or other security failures. 7. Perform tests on a periodic basis on the effectiveness of the implemented physical, technical and administrative safeguards.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		8. Perform risk assessments or third-party validations on a periodic basis that include the implemented physical, technical and administrative safeguards and review the results of the assessment or third-party validation for remediation.
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	*Security Safeguards* 1. Maintain a written information security policy. 2. Implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. 3. Communicate to employees their obligations and the importance of maintaining the security of personal information. 4. Require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. Such requirement should include: a. Implementing an information security program that is proportionate to the sensitivity of the information and services provided b. Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information c. Taking immediate steps to correct/address the security failure which caused the privacy or security breach

Question	Assessment Criteria	Schellman Minimum Certification Requirement
caused the privacy or security breach?		

ACCESS AND CORRECTION

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

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

Question	Assessment Criteria	Schellman Minimum Certification Requirement
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with	*Access** 1. Provide individuals the ability to obtain confirmation of whether or not personal information is held about the requesting individual. 2. If requested, provide individuals access to their personal information. Prior to providing access, confirm the identity of the individual requesting access. Provide access within a reasonable time frame following the request, communicate when the requested access will be granted and communicate the information in a reasonable manner that is generally understandable, in a legible format and compatible with the regular form of interaction with the individual.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
	this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*Access** 1. Provide individuals the ability to obtain confirmation of whether or not personal information is held about the requesting individual. 2. If requested, provide individuals access to their personal information. Prior to providing access, confirm the identity of the individual requesting access. Provide access within a reasonable time frame following the request and communicate the information in a reasonable manner that is generally understandable, in a legible format and compatible with the regular form of interaction with the individual. 3. If a fee is charged for providing access, the fees should not be excessive.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
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 on what the fee is based and how you ensure that the fee is not excessive.		
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented 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,	Where the Applicant 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 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 answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*Integrity of Personal Information* 1. Personal information must be accurate, complete and kept up-to date to the extent necessary for the purposes of use. 2. Provide individuals the ability to challenge the accuracy of their personal information and to have it rectified, completed, amended and/or deleted and ensure procedures are in place to complete the request including communication and confirmation of the request to processors, agent, or other service providers to whom the personal information was transferred. Access and correction mechanisms must be presented in a clear and conspicuous manner. The request should be completed within a reasonable time frame following the request and confirmation should be provided that the request has been completed. 3. If correction is denied, an explanation should be provided, together with contact information for further inquiries about the denial of access or correction 4. Require 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 and ensure procedures are in place to complete the correction. *Access**

Question	Assessment Criteria	Schellman Minimum Certification Requirement
addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the 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?		1. Provide individuals the ability to obtain confirmation of whether or not personal information is held about the requesting individual. 2. If requested, provide individuals access to their personal information. Prior to providing access, confirm the identity of the individual requesting access. Provide access within a reasonable time frame following the request and communicate the information in a reasonable manner that is generally understandable, in a legible format and compatible with the regular form of interaction with the individual. 3. If a fee is charged for providing access, the fees should not be excessive. 4. If the individual is denied access, an explanation must be provided as to why access was denied and provide the appropriate contact information for challenging the denial of access where appropriate.

ACCOUNTABILITY

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question	Assessment Criteria	Schellman Minimum Certification Requirement
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) • Contracts • Compliance with applicable industry or sector laws and regulations • Compliance with self-regulatory applicant code and/or rules • Other (describe)	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	*Accountability* 1. Implement measures to ensure compliance with the APEC Information Privacy Principles.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	*Accountability* 1. Implement measures to ensure compliance the APEC Information Privacy Principles. 2. Appoint an individual(s) to be responsible for overall compliance with the Privacy Principles. 3. Implement procedures to receive, investigate, and respond to privacy-related complaints as well as an explanation of any remedial action where applicable.
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	*Accountability* 1. Implement measures to ensure compliance with the APEC Information Privacy Principles. 2. Appoint an individual(s) to be responsible for overall compliance with the Privacy Principles. 3. Implement procedures to receive, investigate, and respond to privacy-related complaints as well as an explanation of any remedial action where applicable. The procedures should include: a. A description of how individuals may submit complaints, b. A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information, and c. A formal complaint-resolution process.
42. Do you have procedures in place to	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to	*Accountability* 1. Implement measures to ensure compliance the APEC Information Privacy Principles.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
ensure individuals receive a timely response to their complaints?	ensure individuals receive a timely response to their complaints. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	2. Appoint an individual(s) to be responsible for overall compliance with the Privacy Principles. 3. Implement procedures to receive, investigate, and respond to privacy-related complaints as well as an explanation of any remedial action where applicable. The procedures should include: a. A description of how individuals may submit complaints, b. A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information, and c. A formal complaint-resolution process. 4. Procedures should ensure individuals receive a timely response to their complaints.
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	*Accountability* 1. Implement measures to ensure compliance with the APEC Information Privacy Principles. 2. Appoint an individual(s) to be responsible for overall compliance with the Privacy Principles. 3. Implement procedures to receive, investigate, and respond to privacy-related complaints as well as an explanation of any remedial action where applicable. The procedures should include: a. A description of how individuals may submit complaints, b. A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information, and c. A formal complaint-resolution process. 4. Procedures should ensure individuals receive a timely response to their complaints.
44. Do you have procedures in place for	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures regarding	*Accountability* 1. Implement measures to ensure compliance with the APEC Information Privacy Principles.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	2. Appoint an individual(s) to be responsible for overall compliance with the Privacy Principles. 3. Implement procedures to receive, investigate, and respond to privacy-related complaints as well as an explanation of any remedial action where applicable. The procedures should include: a. A description of how individuals may submit complaints, b. A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information, and c. A formal complaint-resolution process. 4. Procedures should ensure individuals receive a timely response to their complaints. 5. Complete formal training with employees that are responsible for carrying out the privacy-related complaints as well as responding to judicial or other government subpoenas, warrants or orders.
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?	Where the Applicant answers **YES, the** Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	*Accountability* 1. Implement measures to ensure compliance the APEC Information Privacy Principles. 2. Appoint an individual(s) to be responsible for overall compliance with the Privacy Principles. 3. Implement procedures to receive, investigate, and respond to privacy-related complaints as well as an explanation of any remedial action where applicable. The procedures should include: a. A description of how individuals may submit complaints, b. A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information, and c. A formal complaint-resolution process.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		4. Procedures should ensure individuals receive a timely response to their complaints. 5. Complete formal training with employees that are responsible for carrying out the privacy-related complaints as well as responding to judicial or other government subpoenas, warrants or orders. 6. Implement procedures for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information.
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 code and/or rules _____ • Other (describe) _____	Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	*Accountability when Personal Information is Transferred* 1. Implement mechanisms with processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that obligations to the individual will be met. The mechanisms should require the following: a. Abide by the APEC-compliant privacy policies and practices as stated in the Privacy Notice or Statement, b. Implement privacy practices that are substantially similar to your policies or privacy practices as stated in the Privacy Notice or Statement, c. Follow instructions provided relating to the manner in which personal information must be handled, d. Impose restrictions on subcontracting unless with your consent, e. CBPRs should be certified by an APEC accountability agent in their jurisdiction, f. Provide self-assessments to ensure compliance with your instructions and/or agreements/contracts.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your APEC-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? _____ • Have their CBPRs certified by an APEC accountability agent	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	*Accountability when Personal Information is Transferred* 2. Implement mechanisms with processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that obligations to the individual will be met. The mechanisms should require the following: a. Abide by the APEC-compliant privacy policies and practices as stated in the Privacy Notice or Statement, b. Implement privacy practices that are substantially similar to your policies or privacy practices as stated in the Privacy Notice or Statement, c. Follow instructions provided relating to the manner in which personal information must be handled, d. Impose restrictions on subcontracting unless with your consent, e. CBPRs should be certified by an APEC accountability agent in their jurisdiction, *Security Safeguards* 1. Maintain a written information security policy. 2. Implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. 3. Communicate to employees their obligations and the importance of maintaining the security of personal information.

Question	Assessment Criteria	Schellman Minimum Certification Requirement
in their jurisdiction? _____ • Notify the Applicant in the case of a breach of the personal information of the Applicant's customers? • Other (describe) _____		4. Require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. Such requirement should include: a. Implementing an information security program that is proportionate to the sensitivity of the information and services provided b. Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information c. Taking immediate steps to correct/address the security failure which caused the privacy or security breach
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.	*Accountability when Personal Information is Transferred* 1. Implement mechanisms with processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that obligations to the individual will be met. The mechanisms should require the following: a. Abide by the APEC-compliant privacy policies and practices as stated in the Privacy Notice or Statement, b. Implement privacy practices that are substantially similar to your policies or privacy practices as stated in the Privacy Notice or Statement, c. Follow instructions provided relating to the manner in which personal information must be handled, d. Impose restrictions on subcontracting unless with your consent,

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		e. CBPRs should be certified by an APEC accountability agent in their jurisdiction, f. Provide self-assessments to ensure compliance with your instructions and/or agreements/contracts.
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 answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	*Accountability when Personal Information is Transferred* 1. Implement mechanisms with processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that obligations to the individual will be met. The mechanisms should require the following: a. Abide by the APEC-compliant privacy policies and practices as stated in the Privacy Notice or Statement, b. Implement privacy practices that are substantially similar to your policies or privacy practices as stated in the Privacy Notice or Statement, c. Follow instructions provided relating to the manner in which personal information must be handled, d. Impose restrictions on subcontracting unless with your consent, e. CBPRs should be certified by an APEC accountability agent in their jurisdiction, f. Provide self-assessments to ensure compliance with your instructions and/or agreements/contracts. 2. Perform regular spot checking or monitoring the processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts
50. Do you disclose personal information to other recipient **persons**	If **YES**, the Accountability Agent must ask the Applicant to explain:	*Accountability when Personal Information is Transferred* 1. Implement mechanisms with processors, agents, contractors, or other service providers pertaining to

Question	Assessment Criteria	Schellman Minimum Certification Requirement
or organisations in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	(1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	personal information they process on your behalf, to ensure that obligations to the individual will be met. The mechanisms should require the following: a. Abide by the APEC-compliant privacy policies and practices as stated in the Privacy Notice or Statement, b. Implement privacy practices that are substantially similar to your policies or privacy practices as stated in the Privacy Notice or Statement, c. Follow instructions provided relating to the manner in which personal information must be handled, d. Impose restrictions on subcontracting unless with your consent, e. CBPRs should be certified by an APEC accountability agent in their jurisdiction, f. Provide self-assessments to ensure compliance with your instructions and/or agreements/contracts. 2. Perform regular spot checking or monitoring the processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts. 3. If personal information is disclosed to other recipient persons or organizations in situations where due diligence and reasonable steps to ensure compliance with the APEC CBPRs by the recipient as described above is impractical or impossible, maintain documentation as to the reason why due diligence and reasonable steps consistent with the above minimum requirements are impractical or impossible to perform. Additionally, implement mechanisms to ensure that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where an individual's consent

Question	Assessment Criteria	Schellman Minimum Certification Requirement
		was obtained for the disclosure, documentation of the consent and how it was obtained must be maintained.

Appendix C: CBPR System Intake Questionnaire

GENERAL

1) Name of the Organization that is seeking certification:
   _____

2) List of subsidiaries and/or affiliates governed by your privacy policy to be covered by this certification, their location, and the relationship of each to you:
   _____

3) Organization's Contact Point for Cross Border Privacy Rules ("CBPR")
   Name: _____
   Title: _____
   Email: _____
   Phone: _____

4) For what type(s) of personal information are you applying for certification? Please check all that apply.

   Customer/ Prospective Customer _____
   Employee/Prospective Employee _____
   Other (Please describe) _____

5) In which economies do you, your affiliates and/or subsidiaries collect or anticipate collecting personal information to be certified under this system? Please check all that apply.

☐ Australia	☐ New Zealand
☐ Brunei Darussalam	☐ Papua New Guinea
☐ Canada	☐ Peru
☐ Chile	☐ Philippines
☐ People's Republic of China	☐ Russia
☐ Hong Kong, China	☐ Singapore
☐ Indonesia	☐ Chinese Taipei
☐ Japan	☐ Thailand
☐ Republic of Korea	☐ United States
☐ Malaysia	☐ Viet Nam
☐ Mexico	

6) To which economies do you, your affiliates and/or subsidiaries transfer or anticipate transferring personal information to be certified under this system? Please check all that apply.

☐ Australia	☐ New Zealand
☐ Brunei Darussalam	☐ Papua New Guinea
☐ Canada	☐ Peru
☐ Chile	☐ Philippines
☐ People's Republic of China	☐ Russia
☐ Hong Kong, China	☐ Singapore
☐ Indonesia	☐ Chinese Taipei
☐ Japan	☐ Thailand

☐ Republic of Korea ☐ Malaysia ☐ Mexico	☐ United States ☐ Viet Nam

NOTICE (QUESTIONS 1-4)

The questions in this section are directed towards:

(a) ensuring that individuals understand your policies regarding personal information that is collected about them, to whom it may be transferred and for what purpose it may to be used; AND

(b) ensuring that, subject to the qualifications listed in part II, individuals know when personal information is collected about them, to whom it may be transferred and for what purpose it may be used.

General

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.

_____ Y _____ N

a) Does this privacy statement describe how your organization collects personal information?

_____ Y _____ N

b) Does this privacy statement describe the purpose(s) for which personal information is collected?

_____ Y _____ N

c) Does this privacy statement inform individuals as to whether and for what purpose you make personal information available to third parties?

_____ Y _____ N

d) Does this privacy statement disclose the name of your company and location, including information on how to contact you about your practices and handling of personal information upon collection? Where YES describe below.

_____ Y _____ N

e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?

_____ Y _____ N

f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?

_____ Y _____ N

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?

_____ Y _____ N

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?

_____ Y _____ N

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?

_____ Y _____ N

Qualifications to the Provision of Notice

The following are situations in which the application at the time of collection of the APEC 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 (QUESTIONS 5-7)

The questions in this section are directed towards ensuring that collection of information is limited to the stated purposes for which it is collected. 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.

5. How do you obtain personal information:

    a) Directly from the individual?

    _____ Y _____ N

    b) From third parties collecting on your behalf?

    _____ Y _____ N

    c) Other. If YES, describe.

    _____ Y _____ N

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?

    _____ Y _____ N

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.

    _____ Y _____ N

USES OF PERSONAL INFORMATION (QUESTIONS 8-13)

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

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.

    _____ Y _____ N

9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below.

a) Based on express consent of the individual?

b) Compelled by applicable laws?

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.

_____ Y _____ N

11. Do you transfer personal information to personal information processors? If YES, describe.

_____ Y _____ N

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? Describe below.

_____ Y _____ N

13. If you answered NO to question 12, or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances?

a) Based on express consent of the individual?

b) Necessary to provide a service or product requested by the individual?

c) Compelled by applicable laws?

CHOICE (QUESTIONS 14-20)

The questions in this section are directed towards ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in "Qualifications to the Provision of Choice Mechanisms".

General

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.

_____ Y _____ N

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.

_____ Y _____ N

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.

_____ _____

Y N

17. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?

_____ _____
Y N

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?

_____ _____
Y N

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 and affordable? Where YES, describe.

_____ _____
Y N

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.

Qualifications to the Provision of Choice Mechanisms

The following are situations in which the application of the APEC 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 (QUESTIONS 21-25)

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

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.

_____ Y _____ N

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.

_____ Y _____ N

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.

_____ Y _____ N

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.

25. Do you require personal information processors, agents, or other service providers who act on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?

_____ Y _____ N

SECURITY SAFEGUARDS (QUESTIONS 26-35)

The questions in this section are directed towards ensuring that when individuals entrust their information to an organization, their information will be protected with reasonable security safeguards to prevent loss or unauthorized access to personal information or unauthorized destruction, use, modification or disclosure of information or other misuses.

26. Have you implemented an information security policy?

_____ Y _____ N

27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?

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.

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).

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:

    a) Employee training and management or other organizational safeguards?

    _____ Y _____ N

    b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?

    _____ Y _____ N

    c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?

    _____ Y _____ N

    d) Physical security?

    _____ Y _____ N

31. Have you implemented a policy for secure disposal of personal information?

_____ Y _____ N

32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?

_____ Y _____ N

33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.

_____ Y _____ N

34. Do you use third-party certifications or other risk assessments? Describe below.

_____ Y _____ N

35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by:

    a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?

    _____ Y _____ N

    b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of your organization's personal information?

    _____ Y _____ N

    c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?

    _____ Y _____ N

ACCESS AND CORRECTION (QUESTIONS 36-38)

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 by which the ability to access and correct information is provided may differ depending on the nature of the information and other interests. For this reason, 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. "Qualifications to the Provision of Access and Correction" sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order.

General

36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.

    _____ Y _____ N

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 organization's policies/procedures for receiving and handling access requests below. Where NO, proceed to question 38

    _____ Y _____ N

a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.

_____ Y _____ N

b) Do you provide access within a reasonable timeframe following an individual's request for access? If YES, please describe.

_____ Y _____ N

c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.

_____ Y _____ N

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.)?

_____ Y _____ N

e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.

_____ Y _____ N

38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your organization's policies/procedures in this regard below and answer questions 38 (a), (b), (c), (d) and (e).

_____ Y _____ N

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.

_____ Y _____ N

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?

_____ Y _____ N

c) Do you make such corrections or deletions within a reasonable timeframe following an individual's request for correction or deletion?

_____ Y _____ N

d) Do you provide a copy of the corrected personal information or provide confirmation that the data has been corrected or deleted to the individual?

_____ Y _____ N

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?

_____ Y _____ N

Qualifications to the Provision of Access and Correction Mechanisms

Although organizations should always make good faith efforts to provide access, there are some situations, described below, in which it may be necessary for organizations 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 (QUESTIONS 39-51)

The questions in this section are directed towards ensuring that you are accountable for complying with measures that give effect to the Principles stated above. Additionally, when transferring information, you should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.

General

39. What measures does your organization take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe below.

- Internal guidelines or policies (if applicable, describe how implemented)
- Contracts _____
- Compliance with applicable industry or sector laws and regulations _____
- Compliance with self-regulatory organization code and/or rules _____
- Other (describe) _____

40. Has your organization appointed an individual(s) to be responsible for your organization's overall compliance with the Privacy Principles?

_____ Y _____ N

41. Does your organization have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.

_____ Y _____ N

42. Does your organization have procedures in place to ensure individuals receive a timely response to their complaints?

_____ Y _____ N

43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.

_____ Y _____ N

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.

_____ Y _____ N

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?

_____ Y _____ N

Maintaining Accountability When Personal Information is Transferred

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 organization code and/or rules* _____
    - *Other (describe)* _____

47. Do these mechanisms generally require that personal information processors, agents, contractors or other service providers:

    - Abide by your APEC-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? _____
- Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____
- Other (describe) _____

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.

_____ Y _____ N

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 below.

_____ Y _____ N

50. Do you disclose personal information to other personal information controllers in situations where due diligence and mechanisms to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?

_____ Y _____ N

Appendix D: Case Notes Template

Information within the case notes will be anonymized when released.

General heading
This section will communicate a clear, concise and straightforward generalization of the case.
Citation
This section will include the following elements: • A descriptor of the case; • The year of publication; • The economy where the Accountability Agent is based (i.e., USA), and; • The unique number assigned to the case.
Case report
This section will include the following elements: • An account of the facts (e.g. as initially asserted on a complaint and as found after investigation); • The elements of the CBPR or PRP program involved in the case; • A discussion of the issues of interest and how the program applied to the facts in question; and • The outcome of the complaint.
Key terms
This section will include the standard terms used in traditional indexing.

Appendix E: Complaint Statistics Template

Complaint Numbers

The total number of complaints will be reported. Where no complaints are received, the complaint statistics template will indicate "none" to ensure it is clear that no complaints were received that year. The number of complaints will be listed by year so that it is clear regarding the number of new complaints received as well as older complaints carried over from the previous reporting period.

To assist readers in understanding the reported figures and to aid in comparability there will be a note that the number reflects an actual and confirmed complaint rather than an inquiry.

Complaint Processing and Outcomes

A description of the process will be outlined.

A listing of the number of the outcomes of each complaint by the following types will be included:

- Complaints received that were outside of the scope of the program requirements or were not covered by the CBPR or PRP programs
- Complaints that were resolved by Schellman
- Complaints transferred to another Accountability Agent, Privacy Enforcement Authority or other enforcement authority
- Complaints received that were incomplete or the complainant was unresponsive to additional information requirements
- Complaints where findings were upheld in part
    - Details about the outcome will be provided including whether enforcement actions were taken
- Complaints where findings were upheld in full
    - Details about the outcome will be provided including whether enforcement actions were taken

Complaints Type

This section will include informative breakdowns of the complaints by type to provide a statistical picture of who is complaining and why.

The complaint types will be listed in the following categories:

- Complaint subject matter broken down by APEC information privacy principle (e.g. notice, collection limitation, use) for CBPR or by security safeguards and/or accountability measures for CBPR;
- Information about complainants, when known, including the economy from which complaints have been made and industry;
- Information about the type of respondents to complaints, including industry classification (e.g. financial service activities, insurance), the capacity in which the respondent falls (e.g. information processor, employer, service provider), and size of company (e.g., small, mid-market, or large).

While some complaints will raise several different issues, the report will provide the basis upon which Schellman is reporting, for example, the principal aspect of the complaint.

Complaints Process Quality Measures

This section will outline how well the complaints resolution system is working. The timeliness of the processing will be reported, including the number or complaints that took longer than the target date to resolve.

General

Schellman will provide a comment on the various figures reported at the end of the reporting period as compared to previous periods to set the statistics in context.

Appendix F: Sampling Guidelines Policy

In some cases, an auditor may need to inspect a sample of documents. Sampling should first validate consistency amongst like systems (build, version, patch levels), employee processes and procedures (through interviews), locations, and requisite documentation. Schellman selects the sample size based on the validated consistency (e.g., number of relevant systems, process events). Where variances or non-compliance occurred, Schellman required additional samples. Sampling guidelines are defined in the table shown below.

Sampling Guidelines

No Exceptions (No areas of Non-Compliance)	Testing Exception(s)/Non-Compliance
Test at least 25% of the population up to a total sample size 25	Increase sample to 40% of the population up to a total sample size of 40

NOTE: Sample testing should be described within the project files.