GLOBAL CBPR FORUM
ACCOUNTABILITY AGENT RECOGNITION APPLICATION

OVERVIEW

*The purpose of this document is to guide the application process for an organization seeking recognition as an Accountability Agent ("**Applicant Accountability Agent**") under the Global Cross-Border Privacy Rules (CBPR) System or Global Privacy Recognition for Processors (PRP) System, or both. This document explains the necessary recognition criteria and provides the program requirements of the Global CBPR and Global PRP Systems ("**Global CBPR System Program Requirements**" and "**Global PRP System Program Requirements**"). Only Accountability Agents recognized by the Global CBPR Forum ("**Forum**") may participate in the Global CBPR and Global PRP Systems. Once recognized, Accountability Agents may publicize this recognition and certify organizations as Global CBPR- and/or Global PRP-compliant. A recognized Accountability Agent would only be able to certify as Global CBPR- and/or Global PRP-compliant those organizations that are subject to enforcement as described in the Policies, Rules and Guidelines.*

APPLICATION PROCESS

In order to be considered eligible for recognition by the Forum, an Applicant Accountability Agent must:

- Explain how it is subject to enforcement by a Privacy Enforcement Authority ("**PEA**") or other relevant enforcement authority of a Member of the Global CBPR Forum ("**Member**"); AND
- Describe how each of the Accountability Agent Recognition Criteria (Annex A) have been met using the Accountability Agent Recognition Criteria Checklist (Annex B); AND
- Agree to make use of the Global CBPR System Intake Questionnaire and/or the Global PRP System Intake Questionnaire to assess Applicant Organizations' compliance with the Global CBPR System Program Requirements and/or the Global PRP System Program Requirements; OR use the Global CBPR System Program Requirements Map (Annex C) and/or the Global PRP System Program Requirements Map (Annex D) to demonstrate how its intake and review processes meet the program requirements, and publish its program requirements; *AND*
- Complete the signature and contact information sheet (Annex G).

The completed signature and contact information sheet and all necessary supporting documentation should be submitted to the relevant government entities in any Member in which the Applicant Accountability Agent intends to operate. The relevant government entities will conduct an initial review to ensure the necessary documentation have been included in the application, or other review as appropriate. They may consult with other government entities where necessary and will forward all information received to the Chair of the Global Forum Assembly ("**GFA**") and the Chair of the Accountability Agent Oversight and Engagement Committee ("**AA Committee**") where appropriate. The AA Committee will review the submitted information (and request additional information as required), when considering recommending the Applicant Accountability Agent for recognition by the Forum as a Global CBPR and/or Global

PRP System Accountability Agent. The AA Committee Chair will communicate the outcome of the application in writing to Applicant Accountability Agents.

Annex A

ACCOUNTABILITY AGENT RECOGNITION CRITERIA

CRITERIA

Conflicts of Interest

1) General Requirements:

   a. An Accountability Agent must be free of actual or potential conflicts of interest in order to participate in the Global CBPR and/or Global PRP Systems. To participate as an Accountability Agent in these Systems, the Accountability Agent must be able to perform all tasks related to an Applicant Organization's certification and ongoing participation in the Global CBPR and/or Global PRP Systems free from influences that would compromise the Accountability Agent's professional judgment, objectivity and integrity.

   b. An Accountability Agent must satisfy the GFA with evidence that internal structural and procedural safeguards are in place to address potential and actual conflicts of interest. Such safeguards should include but not be limited to:

      i. Written policies for disclosure of potential conflicts of interest and, where appropriate, withdrawal of the Accountability Agent from particular engagements. Such withdrawal will be required in cases where an Accountability Agent is related to an organization (1) seeking certification as Global CBPR- and/or Global PRP-compliant ("**Applicant Organization**"), or (2) maintaining certification as Global CBPR- and/or Global PRP-compliant ("**Certified Organization**"), to the extent that it would give rise to a risk that the Accountability Agent's professional judgment, integrity, or objectivity could be influenced by the relationship;

      ii. Written policies for internal review of potential conflicts of interest with Applicant Organizations and Certified Organizations;

      iii. Written policies governing the separation of personnel handling privacy certification functions from personnel handling sales and consulting functions;

      iv. Published program requirements for Applicant Organizations and Certified Organizations (see paragraph 4 "Program Requirements");

v. Mechanisms for regular reporting to the relevant government entity on certification of new Applicant Organizations, audits of existing Certified Organizations, and dispute resolution; and

vi. Mechanisms for mandatory publication of case reports in certain circumstances.

2) Requirements with respect to particular Applicant Organizations and/or Certified Organizations

a. At no time may an Accountability Agent have a direct or indirect affiliation with any Applicant Organization or Certified Organization that would prejudice the ability of the Accountability Agent to render a fair decision with respect to that organization's certification and ongoing participation in the Global CBPR and/or Global PRP Systems, including but not limited to during the application review and initial certification process; during ongoing monitoring and compliance review; during re-certification and annual attestation; and during dispute resolution and enforcement of the program requirements against a Certified Organization. Such affiliations, which include but are not limited to the Applicant Organization or Certified Organization and the Accountability Agent being under common control such that the Applicant Organization or Certified Organization can exert undue influence on the Accountability Agent, constitute relationships that require withdrawal under 1(b)(i).

b. For other types of affiliations that may be addressed by structural safeguards or other procedures undertaken by the Accountability Agent, the existence of any such affiliations between the Accountability Agent and the Applicant Organization or Certified Organization must be disclosed promptly to the AA Committee, together with an explanation of the safeguards that are in place to ensure that such affiliations do not compromise the Accountability Agent's ability to render a fair decision with respect to such an Applicant Organization or Certified Organization. Such affiliations include but are not limited to:

i. officers of the Applicant Organization or Certified Organization serving on the Accountability Agent's board of directors in a voting capacity, and vice versa;

ii. significant monetary arrangements or commercial relationship between the Accountability Agent and the Applicant Organization or Certified Organization, outside of the fee charged for certification and participation in the Global CBPR and/or Global PRP Systems; or

iii. all other affiliations which might allow the Applicant Organization or Certified Organization to exert undue influence on the Accountability Agent regarding the Applicant Organization's

certification and participation in the Global CBPR and/or Global PRP Systems.

c. Outside of the functions described in paragraphs 5-14 of this Annex A, an Accountability Agent will refrain from performing for its Certified Organizations or Applicant Organizations services that are related to their certification, on-going participation in the Global CBPR and/or Global PRP System or their data privacy practices and procedures for a fee or any interest or benefit. Such services include but are not limited to:

   i. consulting or technical services related to the development or implementation of a Certified Organization's or Applicant Organization's data privacy practices and procedures;

   ii. consulting or technical services related to the development of a Certified Organization's or Applicant Organization's privacy policy or statement; or

   iii. consulting or technical services related to a Certified Organization's or Applicant Organization's security safeguards.

d. An Accountability Agent may be engaged to perform consulting or technical services for an Applicant Organization or Certified Organization other than services relating to their certification and on-going participation in the Global CBPR and/or Global PRP Systems. Where this occurs, the Accountability Agent will disclose to the AA Committee:

   i. the existence of the engagement; and

   ii. an explanation of the safeguards in place to ensure that the Accountability Agent remains free of actual or potential conflicts of interest arising from the engagement [*such safeguards may include segregating the personnel providing the consulting or technical services from the personnel performing the functions described in paragraphs 5 -14 of this Annex A*].

e. Provision of services as required in paragraphs 3 through 6 shall not be considered performing consulting services which might trigger a prohibition contained in this document.

3) In addition to disclosing to the AA Committee all withdrawals described above in paragraph 1(b)(i), an Accountability Agent also shall disclose to the AA Committee those activities or business ventures identified in paragraph 1(b) above that might on their face have been considered a conflict of interest but did not result in withdrawal. Such disclosures should include a description of the reasons for non-withdrawal and the measures the Accountability Agent took to avoid or address any potential prejudicial results stemming from the actual or potential conflict of interest.

Program Requirements

4) An Accountability Agent evaluates Applicant Organizations against the Global CBPR and/or Global PRP Program Requirements ("**Program Requirements**"). (*NOTE*: an Accountability Agent may charge a fee to a Certified Organization for provision of these services without triggering the prohibitions contained in paragraph 1 or 2.)

Certification Process

5) An Accountability Agent has a comprehensive process to review an Applicant Organization's policies and practices with respect to the Applicant Organization's participation in the Global CBPR and/or Global PRP Systems and to verify its compliance with the Program Requirements. The certification process includes:

    a. An initial assessment of compliance, which will include verifying the contents of the Global CBPR and/or Global PRP Intake Questionnaires completed by the Applicant Organization against the Program Requirements, and which may also include in-person or phone interviews, inspection of the personal data system, website scans, or automated security tools;

    b. A comprehensive report to the Applicant Organization outlining the Accountability Agent's findings regarding the Applicant Organization's level of compliance with the Program Requirements. Where non- fulfilment 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 Global CBPR and/or Global PRP Systems;

    c. Verification that any changes required under paragraph 5(b) have been properly completed by the Applicant Organization;

    d. Certification that the Applicant Organization is in compliance with the Program Requirements; and

    e. Provision of the relevant details of the Certified Organization's certification for the Forum's Compliance Directory. The relevant details should include at least the following: the name of the Certified Organization, links to the Certified Organization's website and privacy policy, contact information, the name of the Accountability Agent that certified the Certified Organization and can handle consumer disputes, the name of the relevant PEA, the scope of the certification, the date that the Certified Organization was first certified, and the expiry date for the current certification.

On-going Monitoring and Compliance Review Processes

6) An Accountability Agent has comprehensive written procedures designed to ensure the integrity of the certification process and to monitor Certified Organizations throughout their certification periods to ensure continued compliance with the Program Requirements.

7) Where there are reasonable grounds for an Accountability Agent to believe that a Certified Organization has engaged in a practice that may constitute a breach of the Program Requirements, the Accountability Agent will trigger an immediate review process and verify the Certified Organization's compliance. Where non-compliance with any of the Program Requirements is found, the Accountability Agent will notify the Certified Organization, outline the corrections that the Certified Organization will need to make, and provide a reasonable timeframe within which these corrections must be completed. The Accountability Agent must verify that the required corrections have been properly completed by the Certified Organization within the stated timeframe.

Re-Certification and Annual Attestation

8) An Accountability Agent will require Certified Organizations to attest on an annual basis to their continued compliance to the Program Requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-certification. Where there has been a material change to the Certified Organization's privacy policy (as reasonably determined by the Accountability Agent in good faith), the Accountability Agent will carry out an immediate review process. This re-certification review process includes:

    a. An assessment of compliance, which will include verification of the contents of the Global CBPR and/or Global PRP Intake Questionnaires completed by the Certified Organization, and which may also include in-person or phone interviews, inspection of the personal data system, website scans, or automated security tools;

    b. A report to the Certified Organization outlining the Accountability Agent's findings regarding the Certified Organization's level of compliance with the Program Requirements. The report must also list any corrections the Certified Organization needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification;

    c. Verification that required corrections have been properly completed by the Certified Organization; and

    d. Notice to the Certified Organization that the Certified Organization is in compliance with the Program Requirements and has been re-certified.

Dispute Resolution Process

9) An Accountability Agent must have a mechanism to receive and investigate complaints about Certified Organizations and to resolve disputes between complainants and Certified Organizations in relation to non-compliance with the Program Requirements, as well as a mechanism for cooperation on dispute resolution with other Accountability Agents when appropriate and where possible. Such mechanism must be publicized on the Certified Organization's website. An Accountability Agent may choose not to directly supply the dispute resolution mechanism. The dispute resolution mechanism

may be contracted out by an Accountability Agent to a third party for supply of the dispute resolution service. Where the dispute resolution mechanism is contracted out by an Accountability Agent, the relationship must be in place at the time the Accountability Agent is recognized under the Global CBPR and/or Global PRP Systems. An Accountability Agent's website must include the contact point information for the relevant PEA(s). Publicizing such contact point information allows consumers or other interested parties to direct questions and complaints to the relevant Accountability Agent, or if necessary, to contact the relevant PEA(s).

10) The dispute resolution process, whether supplied directly or by a third party under contract, includes the following elements:

    a. A process for receiving complaints and determining whether a complaint concerns the Certified Organization's obligations under the Global CBPR and/or Global PRP Systems, and that the filed complaint falls within the scope of the relevant Program Requirements;

    b. A process for notifying the complainant of the determination made under paragraph 10(a), above;

    c. A process for investigating complaints;

    d. A confidential and timely process for resolving complaints. Where non-compliance with any of the Program Requirements is found, the Accountability Agent or contracted third party supplier of the dispute resolution service will notify the Certified Organization outlining the corrections the Certified Organization needs to make and the reasonable timeframe within which the corrections must be completed;

    e. Written notice of complaint resolution by the Accountability Agent or contracted third party supplier of the dispute resolution service to the complainant and the Certified Organization;

    f. A process for obtaining an individual's consent before sharing that individual's personal information with the relevant PEA(s) and other government entities in connection with a request for assistance;

    g. A process for making publicly available statistics on the types of complaints received by the Accountability Agent or contracted third party supplier of the dispute resolution service and the outcomes of such complaints, and for communicating that information to the relevant PEA(s) and other government entities (see Annex F).

    h. A process for releasing in anonymised form, case notes on a selection of resolved complaints related to the Global CBPR System illustrating typical or significant interpretations and notable outcomes (see Annex E).

Mechanism for Enforcing Program Requirements

11) An Accountability Agent has the authority to enforce its program requirements against Certified Organizations, either through contract or by law.

12) An Accountability Agent has a process in place for notifying Certified Organizations immediately of non-compliance with the Program Requirements and for requiring Certified Organizations to remedy the non-compliance within a specified time period.

13) An Accountability Agent has processes in place to impose the following penalties, which is proportional to the harm or potential harm resulting from the violation, in cases where a Certified Organization has not complied with the Program Requirements and has failed to remedy the non-compliance within a specified time period. [*NOTE*: In addition to the penalties listed below, Accountability Agent may execute contracts related to legal rights and, where applicable, those related intellectual property rights enforceable in a court of law.]

    a. Requiring Certified Organizations to remedy the non-compliance within a specified time period, failing which the Accountability Agent shall terminate the Certified Organization's certification.

    b. Temporarily suspending the Certified Organization's right to display the Accountability Agent's seal.

    c. Naming the Certified Organization and publicizing the non-compliance.

    d. Referring the violation to the relevant PEA(s). [*NOTE*: this should be reserved for circumstances where a violation raises to the level of a violation of applicable law.]

    e. Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent.

14) An Accountability Agent will refer a matter to the appropriate PEA(s) and other relevant government entities for review and possible law enforcement action, where the Accountability Agent has a reasonable belief pursuant to its established review process that a Certified Organization's failure to remedy a non-compliance with the Program Requirements within a reasonable time (under the procedures established by the Accountability Agent pursuant to paragraph 12) can be a violation of applicable law.

15) Where possible, an Accountability Agent will respond to requests from PEAs and other relevant government entities of a Member that reasonably relate to that Member and to the Global CBPR or Global PRP Systems-related activities of the Accountability Agent.

Annex B

ACCOUNTABILITY AGENT RECOGNITION CRITERIA CHECKLIST

Conflicts of Interest

1) An Applicant Accountability Agent should describe how 1(a) and (b) of Annex A have been met and submit all applicable written policies and documentation.

2) An Applicant Accountability Agent should submit an overview of its internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A.

3) An Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

Program Requirements

4) An Applicant Accountability Agent should indicate whether it intends to use the Global CBPR System Intake Questionnaire and Program Requirements and/or the Global PRP System Intake Questionnaire and Program Requirements, or use Annex C and/or Annex D to map its existing intake and review processes to the Program Requirements.

Certification Process

5) An Applicant Accountability Agent should submit a description of how 5(a)-(d) of Annex A have been met.

On-going Monitoring and Compliance Review Processes

6) An Applicant Accountability Agent should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the Certified Organization's compliance with the Program Requirements described in 5 (a)-(d) of Annex A.

7) An Applicant Accountability Agent should describe the review process to be used in the event of a suspected breach of the Program Requirements described in 5(a)-(d) of Annex A.

Re-Certification and Annual Attestation

8) An Applicant Accountability Agent should describe its re-certification and review process as identified in 8(a)-(d) of Annex A.

Dispute Resolution Process

9) An Applicant Accountability Agent should describe the mechanism to receive and investigate complaints and the mechanism for cooperation with other Accountability Agents that may be used when appropriate.

10) An Applicant Accountability Agent should describe how the dispute resolution process meets the 10(a)-(h) of Annex A, whether supplied directly by itself or by a third party under contract (and if applicable, identify the third party supplier of such services and how this supplier meets the conflict of interest criteria in 1-3 of Annex A) as well as its process to submit the required information in Annexes E and F.

Mechanism for Enforcing Program Requirements

11) An Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against Certified Organizations.

12) An Applicant Accountability Agent should describe the policies and procedures for notifying a Certified Organization of non-compliance with the Program Requirements and provide a description of the processes in place to ensure the Certified Organization remedies the non-compliance.

13) An Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties in 13(a)-(e) of Annex A.

14) An Applicant Accountability Agent should describe its policies and procedures for referring matters to the appropriate PEA(s) and relevant government entities for review and possible law enforcement action. [*NOTE*: immediate notification of violations may be appropriate in some instances.]

15) An Applicant Accountability Agent should describe its policies and procedures to respond to potential requests from PEAs and relevant government entities of Members.

Annex C

GLOBAL CROSS-BORDER PRIVACY RULES SYSTEM (CBPR) PROGRAM REQUIREMENTS MAP

NOTICE

Assessment Purpose – *To ensure that individuals understand the applicant's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. The list of acceptable Qualifications to the Provision of Notice is below.*

Question	Assessment Criteria	Relevant Program 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 Organization's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant Organization's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified); • Is in accordance with the principles of the Global CBPR Framework; • Is easy to find and accessible; • Applies to all personal information, whether collected online or offline; and • States an effective date of privacy statement publication. Where Applicant Organization answers **NO to question 1** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organization that Notice as described herein is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	
1.a) Does this privacy statement describe how personal information is collected?	If **YES**, the Accountability Agent must verify that: • The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant Organization. • 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 Organization that Notice as described herein is required for compliance with this Privacy Principle.	
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must notify the Applicant Organization that notice of the purposes for which personal information is collected is required and must be included in their privacy statement. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization notifies individuals that their personal information will or may be made available to third parties, **identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available.** Where the Applicant Organization answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must notify the Applicant Organization that notice that personal information will be available to third parties is required and must be included in their privacy statement. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	

1.d) Does this privacy statement disclose the name of the Applicant Organization's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization provides name, address and a **functional** e-mail address. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organization that such disclosure of information is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization'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 Organization answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organization, that such information is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the privacy statement includes: • The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). • The process that an individual must follow in order to correct his or her personal information.	

	Where the Applicant Organization answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organization that providing information about access and correction, including the Applicant Organization's typical response times for access and correction requests, is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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 Organization answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization that the notice that personal information is being collected is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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 Organization's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	

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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must determine whether the applicable Qualification is justified.	

Qualifications to the Provision of Notice

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

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

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

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

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

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

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

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

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

COLLECTION LIMITATION

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

Question	Assessment Criteria	Relevant Program 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 Organization indicates from whom they obtain personal information. Where the Applicant Organization answers **YES to any of these sub-parts**, the Accountability Agent must verify the Applicant Organization'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 Organization that it has incorrectly completed the questionnaire.	
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 Organization 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 Organization to identify: • Each type of data collected; • The corresponding stated purpose of collection for each; • All uses that apply to each type of data; and • An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection. Using the above, the Accountability Agent will verify that the Applicant Organization limits the amount and type of personal information to that which is relevant to fulfill the stated purposes. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization 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 Organization answers **YES,** the Accountability Agent must require the Applicant Organization 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 Organization answers **NO**, the Accountability Agent must inform that Applicant Organization that lawful and fair procedures are required for compliance with this Privacy Principle.	

USES OF PERSONAL INFORMATION

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

Question	Assessment Criteria	Relevant Program Requirements
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Where the Applicant Organization 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 Organization's privacy statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Organization Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	

9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual? 9.b) Compelled by applicable laws?	Where the Applicant Organization answers **NO** to question 8, the Applicant Organization must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the Applicant Organization selects 9a, the Accountability Agent must require the Applicant Organization to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant Organization's use of the personal information is based on express consent of the individual (9.a), such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant Organization answers 9.a, the Accountability Agent must require the Applicant Organization 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 Organization selects 9.b, the Accountability Agent must require the Applicant Organization to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant Organization does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant Organization that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this Privacy Principle.	

10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.	Where the Applicant Organization 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 Organization to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g., order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant Organization's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	
11. Do you transfer personal information to personal information processors? If YES, describe.		
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.		
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 Organization answers **NO** to question 13, the Applicant Organization must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant Organization answers **YES** to 13.a, the Accountability Agent must require the Applicant Organization 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 Organization answers **YES** to 13.b, the Accountability Agent must require the Applicant Organization to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant Organization answers **YES** to 13.c, the Accountability Agent must require the Applicant Organization to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant Organization must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant Organization is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant Organization answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant Organization that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this Privacy Principle.	

CHOICE

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

Question	Assessment Criteria	Relevant Program Requirements
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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 Organization answers **NO**, the Applicant Organization must identify the applicable Qualification and the Accountability Agent must verify whether the applicable Qualification is justified. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification the Accountability Agent must inform the Applicant Organization that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	

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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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 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 Organization answers **NO**, the Applicant Organization 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 Organization answers **NO** and does not identify an acceptable Qualification, the Accountability Agent must inform the Applicant Organization a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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 Organization'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 Organization answers **NO**, the Applicant Organization must identify the applicable Qualification and provide a description and the Accountability Agent must verify whether the applicable Qualification is justified. Where the Applicant Organization answers **NO** and does not identify an acceptable Qualification, the Accountability Agent must inform the Applicant Organization that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization's choice mechanism is displayed in a clear and conspicuous manner. Where the Applicant Organization answers **NO**, or when the Accountability Agent finds that the Applicant Organization's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant Organization 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 Privacy Principle.	
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization's choice mechanism is clearly worded and easily understandable.	

	Where the Applicant Organization answers **NO**, and/or when the Accountability Agent finds that the Applicant Organization's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant Organization that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this Privacy Principle.	
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization's choice mechanism is easily accessible and affordable. Where the Applicant Organization answers **NO**, or when the Accountability Agent finds that the Applicant Organization's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant Organization 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 Privacy Principle.	
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant Organization does have mechanisms in place, the Accountability Agent must require the Applicant Organization 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 Organization does not have mechanisms in place, the Applicant Organization 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 Organization answers **NO** and does not provide an acceptable Qualification, the Accountability Agent must inform the Applicant Organization that a mechanism to ensure that choices, when offered, can be honored, must be provided.	

Qualifications to the Provision of Choice Mechanisms

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

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

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

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

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

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

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

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

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

INTEGRITY OF PERSONAL INFORMATION

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

Question	Assessment Criteria	Relevant Program Requirements
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 Organization answers **YES**, the Accountability Agent must require the Applicant Organization to provide the procedures the Applicant Organization 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 Organization to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use**. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this Privacy Principle.	
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 Organization answers **YES**, the Accountability Agent must require the Applicant Organization to provide the procedures and steps the Applicant Organization 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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this Privacy Principle.	
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 Organization answers **YES**, the Accountability Agent must require the Applicant Organization to provide the procedures the Applicant Organization 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 Organization'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 Organization's behalf. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this Privacy Principle.	

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 Organization answers **YES**, the Accountability Agent must require the Applicant Organization to provide the procedures the Applicant Organization 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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this Privacy Principle.	
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 Organization answers **YES**, the Accountability Agent must require the Applicant Organization to provide the procedures the Applicant Organization 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 Organization 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 Organization and by the processors, agents or other service providers. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this Privacy principle.	

SECURITY SAFEGUARDS

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

Question	Assessment Criteria	Relevant Program Requirements
26. Have you implemented an information security policy?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that the implementation of a written information security policy is required for compliance with this Privacy Principle.	
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 Organization provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • **Authentication and access control (e.g., password protections)** • **Encryption** • **Boundary protection (e.g., firewalls, intrusion detection)** • **Audit logging** • **Monitoring (e.g., external and internal audits, vulnerability scans)** • **Other (specify)**	

	The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization'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. 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 Organization 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 Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant Organization that the implementation of such safeguards is required for compliance with this Privacy Principle.	
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 Organization 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 Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization'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.	
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 Organization's employees are aware of the importance of, **and obligations respecting**, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees, • Regular staff meetings or other communications, • Security policy signed by employees, or • Other (specify). Where the Applicant Organization 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 Organization that the existence of such procedures is required for compliance with this Privacy Principle.	
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:	Where the Applicant Organization answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence of each of the safeguards.	

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?	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 Organization must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant Organization answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant Organization that the existence of safeguards on each category is required for compliance with this Privacy Principle.	
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant Organization answers **NO**, the Accountability Agent must inform Applicant Organization that the existence of a policy for the secure disposal of personal information is required for compliance with this Privacy Principle.	
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant Organization answers **NO,** the Accountability Agent must inform the Applicant Organization that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this Privacy Principle.	
33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant Organization adjusts their security safeguards to reflect the results of these tests.	

34. Do you use **third- party certifications or other risk assessments**? Describe below.	The Accountability Agent must verify that such **risk assessments or certifications** are undertaken at appropriate intervals, and that the Applicant Organization 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 Organization and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	
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 Organization's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?	The Accountability Agent must verify that the Applicant Organization 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 Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	

ACCESS AND CORRECTION

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

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. The Qualifications to the Provision of Access and Correction Mechanisms are listed below and set out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order.

Question	**Assessment Criteria**	**Relevant Program Requirements**
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization has procedures in place to respond to such requests. The Applicant Organization 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 Organization'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 Organization must provide the individual with a time frame indicating when the requested access will be granted.	

	Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization 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 Organization'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 regular form of interaction with the individual (e.g., email, same language, etc.)?	Where the Applicant Organization answers **YES,** the Accountability Agent must verify each answer provided. The Applicant Organization 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 Organization 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 Organization answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization that it may be required to permit access by individuals to their personal information. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	

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 Organization's policies/procedures in this regard below and answer questions 38 (a) – (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 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?	Where the Applicant Organization 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 Organization 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 Organization answers **NO** to questions 38(a) – (e) and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	

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?		

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

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

Question	Assessment Criteria	Relevant Program Requirements
39. What measures do you take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____ • Compliance with self- regulatory Applicant Organization code and/or rules ___ • Other (describe) ___	The Accountability Agent has to verify that the Applicant Organization indicates the measures it takes to ensure compliance with the Global CBPR Privacy Principles.	

40. Have you appointed an individual(s) to be responsible for your overall compliance with the Global CBPR Privacy Principles?	Where the Applicant Organization answers **YES,** the Accountability Agent must verify that the Applicant Organization has designated an employee(s) who is responsible for the Applicant Organization's overall compliance with these Privacy Principles. The Applicant Organization must designate an individual or individuals to be responsible for the Applicant Organization'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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that designation of such an employee(s) is required for compliance with this Privacy Principle.	
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant Organization answers **YES,** the Accountability Agent must verify that the Applicant Organization 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 Organization (e.g., Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant Organization's compliance with the Global CBPR 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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.	
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant Organization answers **YES,** the Accountability Agent must verify that the Applicant Organization has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.	
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 Organization indicates what remedial action is considered.	
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant Organization 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 Organization that the existence of such procedures is required for compliance with this Privacy Principle.	

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 Organization answers **YES,** the Accountability Agent must verify that the Applicant Organization 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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that such procedures are required for compliance with this Privacy Principle.	
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 Organization code and/or rules _____ • Others (describe) _____ _____	Where the Applicant Organization answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that implementation of such agreements is required for compliance with this Privacy Principle.	

47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your Global CBPR-compliant privacy policies and practices as stated in your privacy statement? _____ • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your privacy statement? ___ • Follow instructions provided by you relating to the manner in which your personal information must be handled? _____ • Impose restrictions on subcontracting unless with your consent? _____ • Be Global CBPR-certified by a Forum-recognized Accountability Agent in their jurisdiction? _____ • Notify the Applicant Organization in the case of a breach of the personal information of the Applicant Organization's customers? • Other (describe) _	The Accountability Agent must verify that the Applicant Organization makes use of appropriate methods to ensure their obligations are met.	

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.	
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 Organization answers **YES**, the Accountability Agent must verify the existence of the Applicant Organization's procedures such as spot checking or monitoring mechanisms. Where the Applicant Organization answers **NO**, the Accountability Agent must require the Applicant Organization to describe why it does not make use of such spot checking or monitoring mechanisms.	
50. Do you disclose personal information to other recipient **persons or organizations** in situations where due diligence and reasonable steps to ensure compliance with the Global CBPR System by the recipient as described above is impractical or impossible?	If **YES**, the Accountability Agent must ask the Applicant Organization to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant Organization for ensuring that the information, nevertheless, is protected consistent with the Global CBPR Privacy Principles. Where the Applicant Organization relies on an individual's consent, the Applicant Organization must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	

Annex D

GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEM PROGRAM REQUIREMENTS MAP

SECURITY SAFEGUARDS

Question ***(to be answered by the Applicant Organization)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Relevant Program Requirement**
1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that the implementation of a written information security policy is required for compliance with this Privacy Principle.	
2. Describe the physical, technical and administrative safeguards that implement your organization's information security policy.	Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (e.g., password protections) • Encryption • Boundary protection (e.g., firewalls, intrusion detection) • Audit logging • Monitoring (e.g., external and internal audits, vulnerability scans) • Other (specify) The Applicant Organization must periodically review and reassess these measures to evaluate their relevance and effectiveness. Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant Organization that the implementation of such safeguards is required for compliance with this Privacy Principle.	

3. Describe how your organization makes employees aware of the importance of maintaining the security of personal information.	The Accountability Agent must verify that the Applicant Organization'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 Organization 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 Organization that the existence of such procedures is required for compliance with this Privacy Principle.	
4. Has your organization implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant that the existence of such measures is required for compliance with this Privacy Principle.	
5. Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant Organization adjusts their security safeguards to reflect the results of these tests.	

6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information?	The Accountability Agent must verify that the Applicant Organization has in place appropriate processes to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information.	
7. Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the existence of procedures for the secure disposal or return of personal information. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this Privacy Principle.	
8. Does your organization use third-party certifications or other risk assessments? Please describe.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant Organization 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 Organization and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	

ACCOUNTABILITY MEASURES

Question ***(to be answered by the Applicant Organization)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Relevant Program Requirement**
9. Does your organization limit its processing of personal information to the purposes specified by the controller?	The Accountability Agent must verify that the Applicant Organization has policies in place to limit its processing to the purposes specified by the controller.	
10. Does your organization have procedures in place to delete, update, and correct information upon request from the controller?	The Accountability Agent must verify that the Applicant Organization has measures in place to delete, update, and correct information upon request from the controller where necessary and appropriate.	
11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of personal information processing? Please describe.	The Accountability Agent must verify that the Applicant Organization indicates the measures it takes to ensure compliance with the controller's instructions.	
12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the Global PRP System?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization has designated an employee(s) who is responsible for the Applicant Organization's overall compliance with the Global PRP System. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that designation of such an employee(s) is required for compliance with the Global PRP System.	

13. Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to handle, or forward to the controller as appropriate, privacy-related complaints or requests. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.	
14. Does your organization notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization has procedures in place for notifying the controller, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that such procedures are required for compliance with this Privacy Principle.	
15. Does your organization have a procedure in place to notify the controller of your engagement of subprocessors?	The Accountability Agent must verify that the Applicant Organization has in place a procedure to notify controllers that the Applicant Organization is engaging subprocessors.	
16. Does your organization have mechanisms in place with subprocessors to ensure that personal information is processed in accordance with your obligations under the Global PRP System? Please describe.	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the existence of each type of mechanism described. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that implementation of such mechanisms is required for compliance with this Privacy Principle.	
17. Do the mechanisms referred to above generally require that subprocessors:	The Accountability Agent must verify that the Applicant Organization makes use of appropriate methods to ensure their obligations are met.	

a) Follow instructions provided by your organization relating to the manner in which personal information must be handled? b) Impose restrictions on further subprocessing? c) Be Global PRP-certified by a Global CBPR Forum-recognized Accountability Agent in their jurisdiction? d) Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts? If **YES**, describe. e) Allow your organization to carry out regular spot checking or other monitoring activities? If **YES**, describe. f) Other (describe)		
18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization has procedures in place for training employees relating to personal information management and the controller's instructions. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that the existence of such procedures is required for compliance with this Privacy Principle.	

Annex E

GLOBAL CBPR SYSTEM ACCOUNTABILITY AGENT CASE NOTES

The Accountability Agent Recognition Criteria for the Global CBPR System require Applicant Accountability Agents to attest that as part of their dispute resolution mechanism they have a process for releasing, in anonymised form, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes.

This document provides a template, with associated guidance and FAQs, to assist Accountability Agents in meeting the above-mentioned requirement.

Objectives of Release of Case Notes

Dispute resolution is an important element of the Global CBPR and Global PRP Systems. The recognition criteria for Accountability Agents include an obligation to release case notes on a selection of resolved complaints related to the Global CBPR System in order to:

- promote understanding and increase transparency about the Global CBPR System;
- aid consistent interpretation of the Global CBPR Privacy Principles and the Global CBPR System;
- provide additional guidance to organizations on the application of the Global CBPR Privacy Principles and the Global CBPR System; and
- promote accountability of those involved in dispute resolution and build stakeholders' trust in the process.

Commentary on the Template

The template is provided as a tool for Accountability Agents. It is acceptable to depart from the template for stylistic reasons by, for example, reordering the elements (e.g., by switching the date and citation to different ends of the note) or adding additional elements. However, it would be difficult to produce a satisfactory case note without the minimum elements mentioned in the template.

General heading

It is possible to combine the general heading and citation into a single heading or adopt a citation that stands in for a general heading. However, unlike a series of law reports directed exclusively at lawyers, case notes are useful as an educational tool for ordinary consumers and businesses. Accordingly, a general heading that communicates a clear straightforward message is recommended.

Citation

It is essential that all those that may wish to refer to a case note can do so by an accepted citation that unambiguously refers to the same note. All case notes should be issued with a citation including the following elements:

- a description of the case;
- the year of publication;
- a standard abbreviation for the accountability authority (including an indicator of which jurisdiction the Accountability Agent is based); and
- a sequential number.

Case report

The style and approach of case reports can differ substantially but there are several elements that almost certainly will appear. These include:

- an account of the facts (e.g., as initially asserted on a complaint and as found after investigation);
- the relevant law (which will include the corresponding elements of the Global CBPR System);
- a discussion of the issues of interest and how the relevant law and elements of the Global CBPR System applied to the facts in question; and
- the outcome of the complaint.

Key terms

It may be useful to include the standard terms used in traditional indexing or which will appear as tags in on-line environments.

CASE NOTE TEMPLATE

General heading
Citation
Case report · Facts · Law · Discussion · Outcome
Date
Key terms Tags

GLOBAL CBPR SYSTEM CASE NOTES FREQUENTLY ASKED QUESTIONS

Q. How many case notes should an Accountability Agent publish?

A. Accountability Agents may find it useful to set targets for how many case notes should be published and make those targets public. In the initial years of an Accountability Agent's operation a greater number of case notes may be warranted so as to assist advisers and to provide reassurance to regulators and others. In later years, when there is a greater body of case notes available, fewer new notes may be needed. As a general guide, an Accountability Agent handling more than 200 complaints a year might aim to publish about 8-10% of that number in case notes in the early years dropping later to, perhaps, 3–5 %. An Accountability Agent handling very few complaints will need to report a greater proportion of its complaints than an Accountability Agent with handling more complaints, which can be more selective.

Q. Which resolved complaints should be selected for case notes?

A. An Accountability Agent may find it useful to adopt standards to be applied in selecting case suitable for reporting. For instance, to ensure that the more serious cases are identified for reporting, criteria might refer to such indicators of systemic impact such as size of monetary settlements or awards. There is a need to report cases including significant or novel interpretations. There is also a value in reporting some typical cases which raise no novel legal issues but which illustrate the Accountability Agent's operation of the Global CBPR System.

Q. Why are case notes typically reported in anonymous form?

A. Case notes seek to illustrate the Accountability Agent's operation of the Global CBPR System, to educate about matters of interpretation and to ensure those handling complaints remain accountable. These objectives do not necessarily require the respondent to be named. The major objective of the complaints system is to resolve consumer disputes. Subject to the requirements of any particular scheme, this is often facilitated by confidential conciliation or mediation between the parties which does not require, and may even be hampered by, naming respondents publicly.

Q. Might it be useful to name respondents sometimes?

A. Sometimes it will be appropriate to name the respondent to a complaint. Indeed, some Accountability Agents might have this as their usual practice. Even Accountability Agents that do not usually name respondents may need to do so sometimes, for instance where the respondent has publicly announced that the Accountability Agent is handling the complaint or that fact has otherwise become a matter of public notoriety. Occasionally, naming a respondent is an intentional part of the complaint outcome (e.g., if the respondent is refusing to cooperate with the investigation or accept the outcome). It will be good practice for Accountability Agents to adopt transparent policies on their practices for naming respondents.

Q. How much detail should appear in the case notes?

A. When publishing case notes in anonymous form, care needs to be taken in publishing details which might inadvertently identify the parties. Anonymity is usually easily achieved through

generalizing factual details. The level of useful detail in a particular case note will depend upon why it has been chosen for reporting. For example, complaints selected for a case note to illustrate a novel matter of legal interpretation will need the legal reasoning to be set out in full detail. By contrast, a case-note illustrating a fairly routine interpretation in an interesting factual-setting will obviously pay more attention to the facts. In the early phases of an Accountability Agent's operation of the Global CBPR System, relatively simple case notes are acceptable to ensure that advisers understand basic concepts but these should be followed by more detailed notes as familiarity with basic concepts is established.

Q. How should Accountability Agents disseminate case notes?

A. Active steps should be taken to make case notes easily available. Useful approaches may include to:

- maintain a distribution list to which copies of case notes are emailed;
- release case notes individually or in batches during the year with accompanying media statements;
- prepare summaries and use these in newsletters to highlight the release of new case notes;
- post case notes on the Accountability Agent’s website with good indexing and retrieval tools;
- distribute electronic copies through RSS feeds;
- integrate case notes into other educative initiatives such as training packages; and
- co-operate in re-publication by legal publishers.

Q. How can Accountability Agents assist in making case notes readily available?

A. The cross-border nature of the Global CBPR System means that case notes will be useful to consumers, businesses, regulators and advisers in a variety of jurisdictions and not just in the Accountability Agent’s home jurisdiction. Extra efforts should be taken to make their case notes widely available. These extra efforts will also contribute to consistency in interpretation globally. Two key steps that Accountability Agents can take to make their case notes accessible include:

- to facilitate the efforts of those who wish to re-publish their case notes; and
- to provide their case notes, in electronic form, to a recognised international consolidated point of access.

Q. How can Accountability Agents facilitate the efforts of those who wish to republish their case notes?

A. Third party publishers can enable case notes to be made more widely available to the public, specialist bodies, advisers, researchers and regulators. Accountability Agents may facilitate re-publication by giving a general license for re-publication of case notes with proper acknowledgement. The general license should be included with the usual copyright statement posted on an Accountability Agent’s website.

Annex F

GLOBAL CBPR AND GLOBAL PRP SYSTEMS ACCOUNTABILITY AGENT COMPLAINT STATISTICS

The Accountability Agent recognition criteria require Applicant Accountability Agents to attest that as part of their dispute resolution mechanism they have a process for releasing complaint statistics and for communicating that information to the PEA(s) and relevant government entities.

This document provides a template, with associated guidance and FAQs to assist Accountability Agents in meeting the above-mentioned requirement.

Objectives of Reporting Complaint Statistics

Dispute resolution is an important element of the Global CBPR and Global PRP Systems. The recognition criteria for Accountability Agents includes an obligation to publish and report statistics on complaints received in order to:

- promote understanding and increase transparency about the Global CBPR and Global PRP Systems;
- aid consistent interpretation of the Global CBPR Privacy Principles and the Global CBPR and Global PRP Systems;
- provide additional guidance to organizations on the application of the Global CBPR Privacy Principles and the Global CBPR and Global PRP Systems; and
- promote accountability of those involved in dispute resolution and build stakeholders' trust in the process.

Commentary on the Template

The template is provided as a tool for Accountability Agents. It is acceptable to depart from the template by reporting additional statistics. However, the core minimum statistics should be reported in each case since they will form a common and comparable minimum data set across all Accountability Agent dispute resolution processes under the Global CBPR and Global PRP Systems. In particular jurisdictions, governmental authorities may require the reporting of additional statistics.

Complaint numbers

The total number of complaints should be reported. Where no complaints are received, the complaint statistics template should be submitted indicating "none" to ensure it is clear that no complaints were received that year. A format for reporting will need to be adopted that makes clear the number of new complaints received as well as older complaints carried over from the previous reporting period.

To assist readers to understand the reported figures and to aid in comparability there should be a note as to how terms are being used. For instance, some matters may be on the

borderline between an enquiry about a company's information practice of concern and a complaint about that practice. Such matters may be quickly sorted out with an explanation to the enquirer or perhaps a telephone call to the company. Some programs may treat all matters as complaints while others may reserve that term for more formal dispute resolution or investigation and have another category for the matters treated less formally.

Complaint outcomes

This part of the template provides a picture of the processing of complaints.

Complaints type

The template asks Accountability Agents to provide informative breakdowns of the complaints by type. This will provide a statistical picture of who is complaining and why.

Some complaints will raise several different issues. The report should explain the basis upon which the Accountability Agent is reporting. One approach is, for example, to identify the principal aspect of the complaint and treat it for statistical purposes as being only about that issue. An alternative is to count and classify all the allegations made in a complaint. If the latter approach is taken, the total number of complaint types will exceed the total number of complaints received and this will need to be explained or it may seem to be an anomaly.

Complaints process quality measures

The statistics give a picture as to how well the complaints resolution system is working. At a minimum, some indication as to timeliness should be reported. At its simplest this might be to highlight the number or complaints that took longer than a target date to resolve (e.g. number of complaints on hand that are older than, say, three months) while some complaints systems may be able to produce a variety of more detailed statistics (e.g. the average time to resolve certain types of complaints). In a more sophisticated system other quality measures may be included and an Accountability Agent might, for example, report against internal targets or industry benchmarks if these are available.

General

The Accountability Agent should comment on the various figures reported. To set the statistics in context, it is useful to include three or four years of figures where these are available.

COMPLAINT STATISTICS TEMPLATE

Complaint Numbers
Number of complaints received during the year with a comment by the Accountability Agent on the significance of the number. A note should explain how the term 'complaint' is being used in the reported statistics.
Complaint Processing and Outcomes
Complaints processed during the year broken down by the outcome. Examples of typical outcomes include: • complaints that could not be handled as they were outside the program's jurisdiction (e.g. against a company that is not certified under the Global CBPR and/or Global PRP Systems); • complaints referred back to a business that are resolved at that point; • complaints settled by the Accountability Agent; • complaints transferred to another Accountability Agent, PEA or other enforcement authority; • complaints for which the Accountability Agent has made a finding (such as complaint dismissed, complaint upheld in part, complaint upheld in full). When the Accountability Agent has made findings upholding complaints, further statistical information should be given about the outcomes and any subsequent enforcement action. The Accountability Agent should include a comment on the significance of the complaint outcomes.
Complaints Type
Further statistics should be provided as to the type of complaints, including the subject matter of the complaint and characterization of the complainants and the respondents. Useful classifications will include: • complaint subject matter broken down by Global CBPR Privacy Principles (notice, collection limitation, use, etc); • basic information about complainants, where known, such as the jurisdiction from which complaints have been made; • information about the type of respondents to complaints – this may include industry classification (e.g. financial service activities, insurance), the capacity in which the respondent falls (e.g. processor, employer, service provider), or size of the company (SME, large company etc). The Accountability Agent should comment on the significance of the reported figures.
Complaints Process Quality Measures
An indication should be given as to about any quality measures used by an Accountability Agent. A typical measure may relate to timeliness. The Accountability Agent should offer a comment upon the figures reported.

COMPLAINT STATISTICS FREQUENTLY ASKED QUESTIONS

Q. Why does the Global CBPR Forum require complaint statistics to be released?

A. Complaints statistics are part of a transparent and accountable dispute resolution system. The statistics will help paint a picture of how the Global CBPR and Global PRP Systems are operating. A number of stakeholders have an interest in seeing such a picture. For example, Certified Organizations within a Global CBPR and Global PRP Systems, consumer advocates and regulators all have interest in knowing what happens in relation to the processing of complaints through an Accountability Agent. Transparency will promote understanding and confidence in the system.

Q. Why do I need to release statistics on all the topics in the template?

A. The template lists a minimum set of statistics that should be reported. To get a complete picture, all the categories of statistics are needed. Furthermore, since these are standard requirements across all Members, the resultant statistics should be reasonably comparable. Over time, a picture should emerge as to how well Global CBPR and Global PRP Systems are working and whether change is desirable.

Q. How should these statistics be presented?

A. The template provides the statistics that should be reported and requires that the Accountability Agent comment upon the significance of the figures. It is recommended that the statistics reported for a particular period should be published alongside the equivalent statistics for previous recent periods. Where available, three or four years' worth of figures should be reported. Accountability Agents are encouraged to put some effort into clearly displaying and explaining the statistics so that stakeholders can better appreciate their significance. For example, clear tables of figures with accompanying graphs are helpful.

Q. Are there steps that can be taken to facilitate comparison across jurisdictions?

A. Accountability Agents are to include a classification in their reported statistics based on the Global CBPR Privacy Principles. This will aid comparison. In classifying respondents to complaints by industry type, it is recommended that the United Nations' International Standard Industrial Classification of All Economic Activities be used or national or regional standards on industry classification that are aligned with that international standard.

Annex G

SIGNATURE AND CONTACT INFORMATION

By signing this document, the signing party attests to the truth of the answers given.

[Signature of person who has authority to commit party to the agreement]	**[Date]**

[Typed name]

[Typed title]

[Typed name of organization]

[Address of organization]

[Email address]

[Telephone number]

The first Global CBPR Forum recognition for an Accountability Agent is valid for one year from the date of recognition. Recognition for the same Accountability Agent will be for two years thereafter. One month prior to the end of the recognition period or as soon as practicable in the event of a material change (e.g., ownership, structure, policies), the Accountability Agent must resubmit this form and any associated documentation to the appropriate government entity or PEA(s).

NOTE: Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law.