Annex B

GLOBAL CBPR SYSTEM PROGRAM REQUIREMENTS: ENFORCEMENT MAP

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

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

Column 1 lists the questions in the intake questionnaire to be answered by an Applicant Organization when seeking Global CBPR certification. Column 2 lists the assessment criteria to be used by a Forum-recognized Accountability Agent when verifying the answers provided in Column 1. Column 3 is for use by the Applicant to explain the enforceability of an Applicant Organization's answers in Column 1. Accountability Agents should be able to enforce the Global CBPR System Program Requirements through law or contract, and a jurisdiction's relevant privacy enforcement authorities should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements. Additional documentation to assist in these explanations may be submitted as necessary.

Contents

NOTICE

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

Question	**Assessment Criteria**	**Enforceability**
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	Paragraph 2 of Article 6, Article 8, Article 9 of the PDPA Personal Information Protection Act (hereinafter "the PDPA") http://law.moj.gov.tw/Eng/LawClass/LawContent.aspx?PCODE=I0050021 Article 16 of the PDPA Enforcement Rules Enforcement Rules of the Personal Information Protection Act (hereinafter "the PDPA Enforcement Rules) http://law.moj.gov.tw/Eng/LawClass/LawContent.aspx?PCODE=I0050022

Question	Assessment Criteria	Enforceability
	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.	Paragraph 2 of Article 6, Article 8, Article 9 of the PDPA Article 16 of the PDPA Enforcement Rules
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	Paragraph 2 of Article 6, Article 8, Article 9 of the PDPA Article 16 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	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.	Paragraph 2 of Article 6, Article 8, Article 9 of the PDPA Article 16 of the PDPA Enforcement Rules
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	Paragraph 2 of Article 6, Article 8, Article 9 of the PDPA Article 16 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	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.	Paragraph 2 of Article 6, Article 8, Article 9 of the PDPA Article 16 of the PDPA Enforcement Rules
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.	Paragraph 2 of Article 6, Article 8, Article 9 of the PDPA Article 16 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	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.	Article 4, Paragraph 2 of Article 6, Article 8, Article 9 of the PDPA Article 7, Article 16 of the PDPA Enforcement Rules
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	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	Article 4, Paragraph 2 of Article 6, Article 8, Article 9 of the PDPA Article 7, Article 16 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
purpose(s) for which personal information is being collected?	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.	Paragraph 2 of Article 6, Article 8, Article 9 of the PDPA Article 16 of the PDPA Enforcement Rules

Qualifications to the Provision of Notice

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

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

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

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

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

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

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

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

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

COLLECTION LIMITATION

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

Question	**Assessment Criteria**	**Enforceability**
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.	Article 4, Article 6, Article 19 of the PDPA Article 7, Article 8, of the PDPA Enforcement Rules
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;	Article 4, Article 6, Article 19 of the PDPA Article 7, Article 8, of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	• 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.	Article 4, Article 5, Article 6, Article 19 of the PDPA Article 7, Article 8, of the PDPA Enforcement Rules

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**	**Enforceability**
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.	Article 4, Article 6, Article 20 of the PDPA Article 7, Article 8, of the PDPA Enforcement Rules
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	Article 6, Article 7, Article 20 of the PDPA Article 9, Article 15 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	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.	

Question	Assessment Criteria	Enforceability
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.	Article 4, Article 6, Article 20, Article 21 of the PDPA Article 7, Article 8, of the PDPA Enforcement Rules
11. Do you transfer personal information to personal information processors? If YES, describe.		Article 4, Article 21 of the PDPA Article 7, Article 8, of the PDPA Enforcement Rules
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.		Article 6, Article 20 of the PDPA
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or	Where Applicant Organization answers **NO** to question 13, the Applicant Organization must clarify under what circumstances it discloses or	Article 6, Article 7, Article 20 of the PDPA

Question	Assessment Criteria	Enforceability
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?	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	Article 9, Article 15 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	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**	**Enforceability**
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	Article 6, Article 7, Article 8, Article 9, Article 19 of the PDPA Article 16 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	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;	Article 6, Article 7, Article 8, Article 9, Article 19, Article 20 of the PDPA Article 15, Article 16 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	• 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	

Question	Assessment Criteria	Enforceability
	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:	Article 6, Article 7, Article 8, Article 9, Article 19, Article 20 of the PDPA Article 15, Article 16 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	• 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	Article 6, Article 7, Article 8, Article 9, Article 19, Article 20, of the PDPA Article 15, Article 16 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	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.	Article 6, Article 7, Article 8, Article 9, Article 19, Article 20, of the PDPA Article 15, Article 16 of the PDPA Enforcement Rules
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	Article 6, Article 7, Article 8, Article 9, Article 19, Article 20, of the PDPA Article 15, Article 16 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	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.	Article 14, Article 15, Article 16 of the PDPA Enforcement Rules

Qualifications to the Provision of Choice Mechanisms

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

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

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

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

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

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

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

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

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

INTEGRITY OF PERSONAL INFORMATION

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

Question	**Assessment Criteria**	**Enforceability**
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.	Article 11 of the PDPA
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.**	Article 11 of the PDPA

Question	Assessment Criteria	Enforceability
	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.	Article 11 of the PDPA
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	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.	Article 11 of the PDPA

Question	Assessment Criteria	Enforceability
information was disclosed? If YES, describe.		
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.	Article 4, Article 11 of the PDPA Article 8 of the PDPA Enforcement Rules

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**	**Enforceability (*to be answered by the Economy*)**
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.	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules
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)**	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability (*to be answered by the Economy*)
	• **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.	

Question	Assessment Criteria	Enforceability (*to be answered by the Economy*)
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.	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules
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	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability (*to be answered by the Economy*)
	training and oversight, the Accountability Agent has to inform the Applicant Organization that the existence of such procedures are 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: 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?	Where the Applicant Organization answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant 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.	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules
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.	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability (*to be answered by the Economy*)
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.	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules
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.	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules
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.	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules

Question	**Assessment Criteria**	**Enforceability** **(*to be answered by the Economy*)**
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.	Article 4, Article 27 of the PDPA Article 8, Article 12 of the PDPA Enforcement Rules

ACCESS AND CORRECTION

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

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

Question	**Assessment Criteria**	**Enforceability**
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.	Article 3, Article 10 of the PDPA

Question	Assessment Criteria	Enforceability
	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	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	Article 3, Article 10 of the PDPA 37. a) Although not explicitly stipulated in PDPA, but some subordinate laws, such as Article 8 of **Regulations Governing Security Measures of the Personal Information File for Non-government Agencies Designated by the Financial Supervisory Commission** (http://law.fsc.gov.tw/law/LawContent.aspx?id=GL000933) and Article 13 of **Regulations Governing the Security Assurance Plan and Processing Method for Personal Data of the Engineering Consulting Industry**

Question	Assessment Criteria	Enforceability
with the individual (e.g., email, same language, etc.)? 37.e) Do you charge a fee for providing access? If YES, describe below what the fee is based and how you ensure that the fee is not excessive.	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.	(https://law.moj.gov.tw/Eng/LawClass/LawContent.aspx?PCODE=D0070242) have stipulated explicitly to take steps to confirm the identity. 37. b) Article 13 of the PDPA 37. c) Regarding matters related to the exercise of rights under Article 3 of the Personal Data Protection Act (PDPA) by a data subject who requests access to their personal data — such as providing the means for the data subject to exercise their rights, informing them of any fees payable, specifying the matters to be explained, and, where there are grounds for refusing the exercise of such rights, recording the reasons and notifying the data subject of the method of such notification —although the Personal Data Protection Act (PDPA) does not explicitly stipulate such procedures, they are specified in other subordinate regulations. For example: Article 8 of the "Regulations Governing the Security Maintenance Plan for Personal Data Files Designated by the Financial Supervisory Commission for Non-Public Agencies," and Article 13 of the "Regulations Governing the Personal Data File Security Maintenance Plan and Processing Measures for Engineering Consulting Firms." 37. d) With regard to the procedures by which a data controller enables a data subject to exercise their rights when requesting access to their personal data, although the Personal Data Protection Act (PDPA) does not expressly

Question	Assessment Criteria	Enforceability
		stipulate such procedures, certain subordinate regulations do provide such requirements. For example: Article 8 of the Regulations Governing the Maintenance of Personal Data File Security for Non-Public Agencies Designated by the Financial Supervisory Commission, and Article 13 of the Regulations Governing the Security Maintenance Plan and Processing Measures for Personal Data Files of Engineering Consulting Firms. 37. e) Article 14 of the PDPA
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	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.	Article 3, Article 11 of the PDPA 38.a) Article 8, Article 9 of the PDPA 38.b) Article 11 of the PDPA 38.c) Article 13 of the PDPA 38.d) Article 11, Article 13 of the PDPA 38.e) Article 13 of the PDPA

Question	Assessment Criteria	Enforceability
confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?	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.	

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**	**Enforceability**
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.	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
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.	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
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.	Although not explicitly stipulated in PDPA, but subordinate laws such as Article 5 of **Regulations Governing Security Measures of the Personal Information File for Non-government Agencies Designated by the National Communications Commission** (https://law.moj.gov.tw/LawClass/Law All.aspx?pcode=K0060104) has stipulated explicitly to set a contact point to receive complaints from individuals.
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	Although the PDPA is not explicitly stipulated, if individuals do not receive a response, they can appeal or report to the relevant enforcement

Question	Assessment Criteria	Enforceability
	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.	agency based on the Administrative Procedure Act or other related rules.
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.	Although the PDPA is not explicitly stipulated, if individuals do not receive a response, they can appeal or report to the relevant enforcement agency based on the Administrative Procedure Act or other related rules.
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.	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules
45. Do you have procedures in place for responding to judicial or other government	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	Article 27 of the PDPA Article 12 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
subpoenas, warrants or orders, including those that require the disclosure of personal information?	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.	Article 8 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
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.	Article 8 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
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.	Article 8 of the PDPA Enforcement Rules
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.	Article 8 of the PDPA Enforcement Rules
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	Article 4, Article 27 of the PDPA Article 8, Article 12 of the PDPA Enforcement Rules

Question	Assessment Criteria	Enforceability
	Organization must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	