Republic of the Philippines
NATIONAL PRIVACY COMMISSION

Manila, 19 August 2019

Ms. Shannon Coe
Chair
Electronic Commerce Steering Group
Asia-Pacific Economic Cooperation

Dear Madam Chair:

I am writing this Letter of Intent to participate in the APEC CBPR System pursuant to Paragraph 2.2 of the "Charter of the APEC Cross-Border Privacy Rules System Joint Oversight Panel" (Charter) on behalf of the Republic of the Philippines.

I confirm that the National Privacy Commission, a Privacy Enforcement Authority in the Philippines, is a participant in the Cross-Border Privacy Enforcement Arrangement after having been admitted last 2017

I likewise confirm the Philippines' intent to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2 of the Charter.

In consideration of the above, please find attached the following:

1. A narrative description of the relevant domestic laws and regulations which may apply to any CBPR certification-related activities of an Accountability Agent operating within the Philippine jurisdiction and the enforcement authority associated with these laws and regulations *(Annex A); AND*

2. The Completed APEC Cross-Border Privacy Rules System Program Requirements Enforcement Map *(Annex B)*

Any inquiry regarding this application should be directed to Atty. Jose Amelito Belarmino II, the Head Executive Assistant of the National Privacy Commission, at jose.belarminoii@privacy.gov.ph

Very truly yours,

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner
National Privacy Commission

Cc:

MR. MICHAEL ROSE
Acting Chair
APEC Data Privacy Subgroup
Asia-Pacific Economic Cooperation

MS. SHANNON COE
Chair
Cross-Border Privacy Rules Joint Oversight Panel
Asia-Pacific Economic Cooperation

ANNEX A

PHILIPPINE DOMESTIC LAWS AND REGULATIONS APPLICABLE TO ACCOUNTABILITY AGENT ACTIVITIES

Accountability Agents operating in the Philippines may be subject to the following domestic laws in respect of their certification activities, as follows:

Accountability Agents (AA) may be established under Philippine laws in the form of a single proprietorship, partnership or a corporation. In whatever form, AAs activities are generally regulated by the Republic Act No. 7394 otherwise known as Consumer Act of the Philippines[1], the Republic Act No. 8293 otherwise known as Intellectual Property Code[2], the Republic Act No. 8792 otherwise known as Electronic Commerce Act[3] and the Republic Act of 3815 otherwise known as Revised Penal Code[4].

Apart from the above-mentioned laws, the following legal frameworks are observed in the transactions of AAs in the Philippines:

In the case of AAs organized as a sole proprietorship or partnerships, the Republic Act No. 386 otherwise known as the Civil Code of the Philippines[5] is the primary law that governs their transactions and relationships.

In the case of AAs organized as a private corporation but not government owned and controlled, the Batas Pambansa Bilang 68 otherwise known as the Corporation Code of the Philippines[6] serves as the regulatory framework for all the requirements of establishing a corporation in the Philippines.

Compliance with the Corporation Code is overseen by the Securities and Exchange Commission, the national government regulatory agency charged with supervision over the corporate sector, the capital market participants, the securities and investment instruments market, and the investing public. Subsequent laws were enacted to encourage investments and more active public participation in the affairs of private corporations and enterprises, and to broaden the SEC's mandates.

Recently enacted laws gave greater focus on the SEC's role to develop and regulate the corporate and capital market toward good corporate governance, protection of investors, widest participation of ownership and democratization of wealth. SEC is likewise the registrar and overseer of the Philippine corporate sector; it supervises

[1] https://www.officialgazette.gov.ph/1992/04/13/republic-act-no-7394-s-1992/, last accessed 15 August 2019
[2] https://www.officialgazette.gov.ph/1997/06/06/republic-act-no-8293/, last accessed 15 August 2019
[3] https://www.officialgazette.gov.ph/2000/06/14/republic-act-no-8792-s-2000/, last accessed 15 August 2019
[4] https://www.officialgazette.gov.ph/1930/12/08/act-no-3815-s-1930/, last accessed 15 August 2019
[5] https://www.officialgazette.gov.ph/1949/06/18/republic-act-no-386/, last accessed 15 August 2019
[6] https://www.officialgazette.gov.ph/1980/05/01/batas-pambansa-bilang-68/, last accessed 15 August 2019

more than 500,000 active corporations and evaluates the financial statements (FS) filed by all corporations registered with it. SEC also develops and regulates the capital market, a crucial component of the Philippine financial system and economy.

AAs should likewise consider the Republic Act No. 10667 otherwise known as the Philippine Competition Act (PCA) , the Philippines's comprehensive legal framework on anti-trust. It protects the well-being of consumers by promoting and protecting competitive markets.

It mandates (a) the creation of the Philippine Competition Commission (PCC), as an independent quasi-judicial body classified as an attached agency to the Office of the President and as the primary Government agency tasked with the implementation of the PCA; (b) the regulation of certain commercial activities associated with free and fair competition in the Philippines, such as anti-competitive agreements, abuse of market dominance, and anti-competitive mergers and acquisitions (M&A); and (c) the establishment of a regulatory framework for the investigation, review and approval, adjudication, enforcement and sanctioning of commercial activities relating to free and fair competition in the Philippines.

In the case of AAs organized as a private corporation but is owned and controlled by the Philippines government, the charter that created them shall primarily govern if it was done through direct act of Congress, with the Corporation Code being suppletory in character.

Under current laws, the Governance Commission for Government Owned and Controlled Corporation regulates activities of GOCCs. It was created under Republic Act No. 10149 (RA No. 10149), otherwise known as the "GOCC Governance Act of 2011," as the central policy-making and regulatory body mandated to safeguard the State's ownership rights and ensure that the operations of GOCCs are transparent and responsive to the needs of the public. It has the following powers:

- oversee the selection and nomination of directors/trustees and maintain the quality of Board Governance;
- institutionalize transparency, accountability, financial viability and responsiveness in corporate performance by monitoring and evaluating GOCCs' performance;
- rationalize the Sector through streamlining, reorganization, merger, as well as recommending to the President of the Philippines the privatization or abolition of a GOCC; and
- establish compensation standards to ensure reasonable and competitive remuneration schemes that attract and retain the right talent.

Lastly, if the AAs are GOCCs organized through the Corporation Code, then the Corporation Code shall govern.

ANNEX B

APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS: ENFORCEMENT MAP

As outlined in the Charter of the APEC Cross Border Privacy Rules (CBPR) System's Joint Oversight Panel (JOP), an APEC Member Economy is considered a Participant in the CBPR System after the Chair of the Electronic Commerce Steering Group (ECSG Chair) has notified the Economy that the following conditions have been met:

(i) The Economy's ECSG delegation, or appropriate governmental representative, submits to the ECSG Chair a letter indicating its intention to participate and confirming that at least one Privacy Enforcement Authority in that Economy is a participant in the APEC Cross Border Privacy Enforcement Arrangement (CPEA);

(ii) The Economy indicates its intention to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2 of the Charter of the JOP;

(iii) The Economy's ECSG delegation, or appropriate governmental representative, after consulting with the JOP, submits to the Chair of the ECSG an explanation of how the CBPR System program requirements may be enforced in that Economy; and

(iv) The JOP submits to the Chair of the ECSG a report as to how the conditions in (i)-(iii) above have been satisfied.

The purpose of Annex B is to assist Economies and the JOP in fulfilling the requirements of items (iii) and (iv):

- *This document provides the baseline program requirements of the APEC Cross Border Privacy Rules (CBPR) System in order to guide the Economy's explanation of how each requirement may be enforced in that Economy; and*
- *The information provided by the Economy will form the basis of the JOP's report.*

Column 1 lists the questions in the intake questionnaire to be answered by an applicant organization when seeking CBPR certification. Column 2 lists the assessment criteria to be used by an APEC-recognized Accountability Agent when verifying the answers provided in Column 1. Column 3 is for use by the Economy's ECSG delegation or appropriate governmental representative when explaining the enforceability of an applicant organization's answers in Column 1. An economy'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 CBPR program requirements. Additional documentation to assist in these explanations may be submitted as necessary. This document is to be read consistently with the qualifications to the provision of notice, the

provision of choice mechanisms, and the provision of access and correction mechanisms found in the CBPR Intake Questionnaire.

The purpose of this Pathfinder document is to provide guidelines to assist certified Accountability Agents as they undertake the APEC CBPR compliance review process in a consistent manner across participating APEC economies.

THE ROLE OF ACCOUNTABILITY AGENTS

Accountability Agents are responsible for receiving an Applicant's Self-Assessment documents, verifying an Applicant's compliance with the requirements of the CBPR system, including meeting the standards set by the APEC Privacy Principles and, where appropriate, assisting the Applicant in modifying its policies and practices to meet the requirements of the CBPR. The Accountability Agent will certify those Applicant deemed to have met the criteria for participation in the APEC CBPR, and will be responsible for monitoring the Participants' compliance with the CBPR system, based on the criteria set out below.

ASSESSMENT CRITERIA FOR MINIMUM COMPLIANCE WITH REQUIREMENTS OF APEC PRIVACY PRINCIPLES

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.*

Question (to be answered by the Applicant)	**Assessment Criteria** (to be verified by the Accountability Agent)	**Enforceability** (to be answered by the Economy) **DATA PRIVACY ACT OF 2012 (Republic Act 10173) and IMPLEMENTING RULES AND REGULATIONS OF DATA PRIVACY ACT OF 2012** Website: https://www.privacy.gov.ph/wp-content/uploads/DPA-of-2012.pdf
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	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on	The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. (**Section 11 of the Data Privacy Act of 2012**) The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)***

hyperlinks to the same.	frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline. • States an effective date of Privacy Statement publication. Where Applicant answers **NO to question 1**, and does not identify an applicable qualification subject to the Qualifications to Notice set out	

	below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
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.	The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Personal information must, be: (a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

	• the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	(b) Processed fairly and lawfully; (c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted; (d) Adequate and not excessive in relation to the purposes for which they are collected and processed; (e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and (f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *Provided,* That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further,* That adequate safeguards are guaranteed by said laws authorizing their processing.

		The personal information controller must ensure implementation of personal information processing principles set out herein. (**Section 11 of the Data Privacy Act of 2012)** Furthermore, Section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals	The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. (**Section 11 of the Data Privacy Act of 2012** *)*

	of the purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)***

1. c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant 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 answers **NO** and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be	Section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

	available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a functional e-mail address. Where the Applicant answers **NO** and does not identify an	The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. (**Section 11 of the Data Privacy Act of 2012** *)* The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose

collection? Where YES describe.	applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)*** Furthermore, Section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.
1. e) Does this privacy statement	Where the Applicant answers **YES**, the	The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public

provide information regarding the use and disclosure of an individual's personal information?	Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the	and adherence to the principles of transparency, legitimate purpose and proportionality. (**Section 11 of the Data Privacy Act of 2012** *)* The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)*** Section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal

	Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.
1. f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant 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	Section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission. Furthermore, Section 16 also provides that data subjects also has the right to dispute the inaccuracy or error in the personal information and have the personal information

	Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: *Provided,* That the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject.
2. Subject to the qualifications listed below, at	Where the Applicant answers YES, the Accountability Agent	The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public

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?	must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable	and adherence to the principles of transparency, legitimate purpose and proportionality. (**Section 11 of the Data Privacy Act of 2012** *)* The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)*** Section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity of: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal

	qualification is justified.	information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached	The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. (**Section 11 of the Data Privacy Act of 2012** *)* The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose

	documents, pop-up window, or other. Where the Applicant answers NO and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)*** Furthermore, Section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers NO and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the	Section 16 of the Data Privacy Act of 2012 enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

	Accountability Agent must determine whether the applicable qualification is justified.	

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 (to be answered by the Applicant)	**Assessment Criteria** (to be verified by the Accountability Agent)	**Enforceability** (to be answered by the Economy)
5. How do you obtain personal information: 5. a) Directly from the individual? 5. b) From third parties collecting on your behalf? 5. c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES** to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Personal information must be collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only; processed fairly and lawfully; accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted; adequate and not excessive in relation to the purposes for which they are collected and processed; retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *Provided,* That personal information collected for other purposes may lie processed for

	Applicant that it has incorrectly completed the questionnaire.	historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further,* That adequate safeguards are guaranteed by said laws authorizing their processing. The personal information controller must ensure implementation of personal information processing principles set out herein.
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: · Each type of data collected · The corresponding stated purpose of collection for each; and · All uses that apply to each type of data · An explanation of the compatibility or relatedness of each	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)***

	identified use with the stated purpose of collection Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	
7. Do you collect personal information (whether directly or through the	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

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.	that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)*** .

Uses of Personal Information

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

Question (to be answered by the Applicant)	**Assessment Criteria** (to be verified by the Accountability Agent)	**Enforceability** (to be answered by the Economy)
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation

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.	information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)***
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual?	Where the Applicant answers **NO** to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose

9.b) Compelled by applicable laws?	provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as: · Online at point of · collection · Via e-mail · Via preference/profile · page · Via telephone · Via postal mail, or · Other (in case, specify) Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The	of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)***

	consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed	

	in this Question, is required for compliance with this principle.	
10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other Personal Data Controllers? If YES, describe.	Where the Applicant answers **YES** in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other Personal Data 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.	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)*** Furthermore, Section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed.

	Also, the Accountability Agent must require the Applicant to identify: each type of data disclosed or transferred; the corresponding stated purpose of collection for each type of disclosed data; and the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	Moreover, the data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission. Section 21 of the Act requires each personal information controller to be responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.

		(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request. Furthermore, NPC Circular 16-02 governs the data sharing involving government agencies.
11. Do you transfer personal information to personal information processors? If YES, describe.		Section 21 of the Act requires each personal information controller to be responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.

		(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request. Furthermore, NPC Circular 16-02 governs the data sharing involving government agencies.
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.		Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation

		to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)*** Furthermore, Section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. Moreover, the data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission. Section 21 of the Data Privacy Act of 2012 states that each personal information controller is responsible for personal information under its control or custody, including

		information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. (b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request. Furthermore, NPC Circular 16-02 governs the data sharing involving government agencies.
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure	Where applicant answers **NO** to question 13, the Applicant must clarify under what circumstances it	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

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?	discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers **YES** to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: · Online at point of collection · Via e-mail · Via preference/profile page · Via telephone · Via postal mail, or · Other (in case, specify)	The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ***(Section 18 of the IRR of Data Privacy Act 2012)*** Furthermore, Section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. Moreover, the data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent

	Where the Applicant answers **YES** to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers **YES** to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or	to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission. Section 21 of the Data Privacy Act of 2012 states that each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. (b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

	disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement or permission. Where the Applicant answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other	Furthermore, NPC Circular 16-02 governs the data sharing involving government agencies.

	compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	

Choice

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

Question (to be answered by the Applicant)	**Assessment Criteria** (to be verified by the Accountability Agent)	**Enforceability** (to be answered by the Economy)
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: · Online at point of collection ·Via e-mail	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Under Section 12 of the Data Privacy Act, Consent is one of the bases for lawful processing of personal information. Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

	·Via preference/profile page ·Via telephone ·Via postal mail, or ·Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified.	Section 19 of the IRR of the Data Privacy Act likewise provides that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn. Section 16 of the Data Privacy Act of 2012 enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

	Where the Applicant answers **NO** and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as:	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Under Section 12 of the Data Privacy Act, Consent is one of the bases for lawful processing of personal information. Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

	· 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.	Section 19 of the IRR of the Data Privacy Act likewise provides that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn. Section 16 of the Data Privacy Act of 2012 enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

	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 answers **NO**, the Applicant must identify the applicable qualification to the	

	provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	
16. Subject to the qualifications described below, do you provide a mechanism for individuals to	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of how	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	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	Under Section 12 of the Data Privacy Act, Consent is one of the bases for lawful processing of personal information. Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so. Section 19 of the IRR of the Data Privacy Act likewise provides that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn. Section 16 of the Data Privacy Act of 2012 enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or

	opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: · disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear	its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

	and conspicuous manner , or compatible with that for which the information was collected.] Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a	

	mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	
17. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner . Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Under Section 12 of the Data Privacy Act, Consent is one of the bases for lawful processing of personal information. Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so. Section 19 of the IRR of the Data Privacy Act likewise provides that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.

	allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	Section 16 of the Data Privacy Act of 2012 enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.
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	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers **NO**, and/or	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Under Section 12 of the Data Privacy Act, Consent is one of the bases for lawful processing of personal information. Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or

information, are they clearly worded and easily understandable?	when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so. Section 19 of the IRR of the Data Privacy Act likewise provides that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn. Section 16 of the Data Privacy Act of 2012 enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Under Section 12 of the Data Privacy Act, Consent is one of the bases for lawful processing of personal information. Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so. Section 19 of the IRR of the Data Privacy Act likewise provides that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn. Section 16 of the Data Privacy Act of 2012 enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into

	comply with this principle.	the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Under Section 12 of the Data Privacy Act, Consent is one of the bases for lawful processing of personal information. Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

	identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	Section 19 of the IRR of the Data Privacy Act likewise provides that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn. Section 16 of the Data Privacy Act of 2012 enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The data subject is entitled to be furnished of the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: the description of the personal information to be entered into the system; purposes for which they are being or are to be processed; scope and method of the personal information processing; the recipients or classes of recipients to whom they are or may be disclosed; methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; the identity and contact details of the personal information controller or its representative; the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

Integrity of personal Information

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

Question (to be answered by the Applicant)	**Assessment Criteria** (to be verified by the Accountability Agent)	**Enforceability** (to be answered by the Economy)
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the	Section 11 of the Data Privacy Act of 2012 states that the processing of personal information shall be allowed, subject to compliance with the requirements of the law and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Section 18 of the Implementing Rules and Regulations of the law states that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

	Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	Furthermore, section 16 of the law enumerated the fundamental rights of the data subjects, one of which is the right to be informed. The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. .
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures and	Section 34 of the IRR of the Data Privacy Act of 2012 states that the data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted

personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that	information by the intended recipients thereof: *Provided*, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.

	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 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,	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure	Section 34 of the IRR of the Data Privacy Act of 2012 states that the data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: *Provided*, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject. Furthermore, section 34 of the IRR states that the data subject also have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system if the personal data is incomplete, outdated, false, or unlawfully obtained; if the personal data is being used for purpose not authorized by the data subject; if the personal data is no longer necessary for the purposes for which they were collected; if the data subject

agents, or other service providers to whom the personal information was transferred? If YES, describe.	that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information	withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing; if the personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized; if the processing is unlawful; if the personal information controller or personal information processor violated the rights of the data subject. The personal information controller may notify third parties who have previously received such processed personal information.

	processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this 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	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational.	Section 34 of the IRR of the Data Privacy Act of 2012 states that the data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: *Provided*, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject. Furthermore, section 34 of the same IRR states that the data subject also have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system if the personal data is incomplete, outdated, false, or unlawfully obtained; if the personal data is being used for purpose not authorized by the data subject; if the personal data is no longer necessary for the purposes for which they were collected; if the data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing; if the personal data

disclosed? If YES, describe.	Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized; if the processing is unlawful; if the personal information controller or personal information processor violated the rights of the data subject. The personal information controller may notify third parties who have previously received such processed personal information.
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure	Section 44 of the IRR of the Data Privacy Act of 2012 states that processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement. The contract or other legal act shall stipulate, in particular, that the personal information processor shall: 1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;

	that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that	2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data; 3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission; 4. Not engage another processor without prior instruction from the personal information controller: *Provided*, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing; 5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights; 6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor; 7. At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing: *Provided*, that this includes deleting existing copies unless storage is authorized by the Act or another law; 8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter; 9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission.

	procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	Section 45 of the same IRR states that the personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.

Security Safeguards

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

Question (to be answered by the Applicant)	**Assessment Criteria** (to be verified by the Accountability Agent)	**Enforceability** (to be answered by the Economy)
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	Section 20 of the Data Privacy Act of 2012 states that the personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:

		1. Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability; 2. A security policy with respect to the processing of personal information; 3. A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and 4. Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach. Furthermore, the law states that the personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision. The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations. The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to

		address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. Section 21 of the law states that each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request. In connection with sensitive personal information maintained by the government, Section22 of the law states that its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein while the Commission shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards.
27. Describe the physical, technical and	Where the Applicant provides a description of the	Section 25 of the IRR of Data Privacy Act of 2012 states that personal information controllers and personal information processors shall implement reasonable and appropriate organizational, physical, and technical security measures for the

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?	physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: · Authentication and access control (eg password protections) Encryption · Boundary protection (eg firewalls, intrusion detection) Audit logging · Monitoring (eg external and internal audits, vulnerability scans) · Other (specify) The Applicant must implement reasonable administrative, technical and physical safeguards, suitable	protection of personal data. The personal information controller and personal information processor shall take steps to ensure that any natural person acting under their authority and who has access to personal data, does not process them except upon their instructions, or as required by law. The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing. These measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. Section 26 of the same IRR states that where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for organizational security: a. Compliance Officers. Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall function as data protection officer, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security. b. Data Protection Policies. Any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organization, physical, and technical security measures, and, for such purpose, take into account the nature, scope,

	to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require	context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects. 1. The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself. 2. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility. 3. The polices shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices. c. Records of Processing Activities. Any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include: 1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing; 2. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;

	information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has NO physical, technical and administrative safeguards, or inadequate safeguards, to protect	3. General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data; 4. A general description of the organizational, physical, and technical security measures in place; 5. The name and contact details of the personal information controller and, where applicable, the joint controller, the its representative, and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security. d. Management of Human Resources. Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data. The said employees, agents, or representatives shall operate and hold personal data under strict confidentiality if the personal data are not intended for public disclosure. This obligation shall continue even after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. There shall be capacity building, orientation or training programs for such employees, agents or representatives, regarding privacy or security policies. e. Processing of Personal Data. Any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review:

	personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	1. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable; 2. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose; 3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems; 4. Policies and procedures for data subjects to exercise their rights under the Act; 5. Data retention schedule, including timeline or conditions for erasure or disposal of records. f. Contracts with Personal Information Processors. The personal information controller, through appropriate contractual agreements, shall ensure that its personal information processors, where applicable, shall also implement the security measures required by the Act and these Rules. It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified in the Act and these Rules, and ensure the protection of the rights of the data subject. Section 27 of the IRR states that where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for physical security:

		1. Policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media; 2. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public; 3. The duties, responsibilities and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time; 4. Any natural or juridical person or other body involved in the processing of personal data shall implement Policies and procedures regarding the transfer, removal, disposal, and re- use of electronic media, to ensure appropriate protection of personal data; 5. Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats. Lastly, section 28 of the same IRR states that where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures: 1. A security policy with respect to the processing of personal data;

		2. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network; 3. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services; 4. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach; 5. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; 6. A process for regularly testing, assessing, and evaluating the effectiveness of security measures; 7. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access
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,	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are	Section 29 of the IRR speaks of the appropriate level of security, it provides that the Commission shall monitor the compliance of natural or juridical person or other body involved in the processing of personal data, specifically their security measures, with the guidelines provided in these Rules and subsequent issuances of the Commission. In determining the level of security appropriate for a particular personal information controller or personal information processor, the Commission shall take into account the nature of the personal data that requires protection, the risks posed by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation. The security measures provided herein shall be subject to regular review and evaluation, and may be updated as necessary by the Commission in

and the context in which it is held.	proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	separate issuances, taking into account the most appropriate standard recognized by the information and communications technology industry and data privacy best practices.

29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: · Training program for employees · Regular staff meetings or other communications · Security policy signed by employees · Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and	Section 26 of the IRR of Data Privacy Act of 2012 states that where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for organizational security: a. Compliance Officers. Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall function as data protection officer, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security. b. Data Protection Policies. Any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organization, physical, and technical security measures, and, for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects. 1. The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself. 2. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility.

	obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	3. The polices shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices. c. Records of Processing Activities. Any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include: 1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing; 2. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing; 3. General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data; 4. A general description of the organizational, physical, and technical security measures in place; 5. The name and contact details of the personal information controller and, where applicable, the joint controller, the its representative, and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

		d. Management of Human Resources. Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data. The said employees, agents, or representatives shall operate and hold personal data under strict confidentiality if the personal data are not intended for public disclosure. This obligation shall continue even after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. There shall be capacity building, orientation or training programs for such employees, agents or representatives, regarding privacy or security policies. e. Processing of Personal Data. Any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review: 1. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable; 2. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose; 3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems; 4. Policies and procedures for data subjects to exercise their rights under the Act;

		5. Data retention schedule, including timeline or conditions for erasure or disposal of records. f. Contracts with Personal Information Processors. The personal information controller, through appropriate contractual agreements, shall ensure that its personal information processors, where applicable, shall also implement the security measures required by the Act and these Rules. It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified in the Act and these Rules, and ensure the protection of the rights of the data subject.
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 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	Section 25 of the IRR of Data Privacy Act of 2012 states that personal information controllers and personal information processors shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data. The personal information controller and personal information processor shall take steps to ensure that any natural person acting under their authority and who has access to personal data, does not process them except upon their instructions, or as required by law. The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing. These measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as

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?	confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.	unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. Section 26 of the same IRR states that where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for organizational security: a. Compliance Officers. Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall function as data protection officer, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security. b. Data Protection Policies. Any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organization, physical, and technical security measures, and, for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects. 1. The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself. 2. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary

		for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility. 3. The polices shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices. c. Records of Processing Activities. Any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include: 1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing; 2. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing; 3. General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data; 4. A general description of the organizational, physical, and technical security measures in place. 5. The name and contact details of the personal information controller and, where applicable, the joint controller, the its representative, and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for

		ensuring compliance with the applicable laws and regulations for the protection of data privacy and security. d. Management of Human Resources. Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data. The said employees, agents, or representatives shall operate and hold personal data under strict confidentiality if the personal data are not intended for public disclosure. This obligation shall continue even after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. There shall be capacity building, orientation or training programs for such employees, agents or representatives, regarding privacy or security policies. e. Processing of Personal Data. Any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review: 1. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable; 2. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose; 3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems; 4. Policies and procedures for data subjects to exercise their rights under the Act;

		5. Data retention schedule, including timeline or conditions for erasure or disposal of records. f. Contracts with Personal Information Processors. The personal information controller, through appropriate contractual agreements, shall ensure that its personal information processors, where applicable, shall also implement the security measures required by the Act and these Rules. It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified in the Act and these Rules, and ensure the protection of the rights of the data subject. Section 27 of the IRR states that where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for physical security: 1. Policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media; 2. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;

		3. The duties, responsibilities and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time; 4. Any natural or juridical person or other body involved in the processing of personal data shall implement Policies and procedures regarding the transfer, removal, disposal, and re- use of electronic media, to ensure appropriate protection of personal data; 5. Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats. Lastly, section 28 of the same IRR states that where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures: 1. A security policy with respect to the processing of personal data; 2. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network; 3. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

		4. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach; 5. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; 6. A process for regularly testing, assessing, and evaluating the effectiveness of security measures; 7. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy	Section 26 of the IRR states that any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review: 1. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable; 2. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose; 3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems; 4. Policies and procedures for data subjects to exercise their rights under the Act;

	for the secure disposal of personal information is required for compliance with this principle.	5. Data retention schedule, including timeline or conditions for erasure or disposal of records.
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	Section 28 of the IRR states that where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures: 1. A security policy with respect to the processing of personal data; 2. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network; 3. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services; 4. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach; 5. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; 6. A process for regularly testing, assessing, and evaluating the effectiveness of security measures; 7. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

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 adjusts their security safeguards to reflect the results of these tests.	Section 26 of the IRR states that any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review: 1. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable; 2. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose; 3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems; 4. Policies and procedures for data subjects to exercise their rights under the Act; 5. Data retention schedule, including timeline or conditions for erasure or disposal of records.
34. Do you use risk assessments or third-party	The Accountability Agent must verify that such risk assessments or	Section 28 of the IRR states that where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:

certifications? Describe below.	certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	1. A security policy with respect to the processing of personal data; 2. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network; 3. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services; 4. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach; 5. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; 6. A process for regularly testing, assessing, and evaluating the effectiveness of security measures; 7. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

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	The Accountablity Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	Section 44 of the IRR states that processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement. The contract or other legal act shall stipulate, in particular, that the personal information processor shall: 1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law; 2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data; 3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission; 4. Not engage another processor without prior instruction from the personal information controller: *Provided*, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing; 5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights; 6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor;

and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?		7. At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing: *Provided*, that this includes deleting existing copies unless storage is authorized by the Act or another law; 8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter; 9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission. Section 45 of the IRR states that the personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller. Furthermore section 20 (f) of the law states that the personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to

		determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. 1. In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information. 2. The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects. 3. The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Access and Correction

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

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

Question	**Assessment Criteria**	Enforceability (to be answered by the Economy)
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests.	Section 34 (a) of the IRR states that the data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling. The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity: 1. Description of the personal data to be entered into the system;

individual? Describe below.	The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the	2. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose; 3. Basis of processing, when processing is not based on the consent of the data subject; 4. Scope and method of the personal data processing; 5. The recipients or classes of recipients to whom the personal data are or may be disclosed; 6. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; 7. The identity and contact details of the personal data controller or its representative; 8. The period for which the information will be stored; and 9. The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission. While Section 34 (c) of the IRR states that the data subject has the right to reasonable access to, upon demand, the following: 1. Contents of his or her personal data that were processed; 2. Sources from which personal data were obtained; 3. Names and addresses of recipients of the personal data; 4. Manner by which such data were processed;

	requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	5. Reasons for the disclosure of the personal data to recipients, if any; 6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject; 7. Date when his or her personal data concerning the data subject were last accessed and modified; and 8. The designation, name or identity, and address of the personal information controller.
37. Upon request, do you provide individuals	Where the Applicant answers **YES** the Accountability Agent	Section 34 (a) of the IRR states that the data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling. The data subject shall be notified and furnished with information indicated hereunder

access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37. a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe. 37. b) Do you provide access	must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate.	before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity: 1. Description of the personal data to be entered into the system; 2. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose; 3. Basis of processing, when processing is not based on the consent of the data subject; 4. Scope and method of the personal data processing; 5. The recipients or classes of recipients to whom the personal data are or may be disclosed; 6. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; 7. The identity and contact details of the personal data controller or its representative; 8. The period for which the information will be stored; and 9. The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission. While Section 34 (c) of the IRR states that the data subject has the right to reasonable access to, upon demand, the following:

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.	Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	1. Contents of his or her personal data that were processed; 2. Sources from which personal data were obtained; 3. Names and addresses of recipients of the personal data; 4. Manner by which such data were processed; 5. Reasons for the disclosure of the personal data to recipients, if any; 6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject; 7. Date when his or her personal data concerning the data subject were last accessed and modified; and 8. The designation, name or identity, and address of the personal information controller.

email, same language, etc)? 37. e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.		
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below	Where the Applicant answers **YES to questions 38.a**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was	Section 34 (d) of the IRR states that the data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: *Provided*, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject. Section 34 (e) of the IRR states that the data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data

and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or	denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant answers **NO** to	from the personal information controller's filing system. This right may be exercised upon discovery and substantial proof of any of the following: 1. The personal data is incomplete, outdated, false, or unlawfully obtained; 2. The personal data is being used for purpose not authorized by the data subject; 3. The personal data is no longer necessary for the purposes for which they were collected; 4. The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing; 5. The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized; 6. The processing is unlawful; 7. The personal information controller or personal information processor violated the rights of the data subject. The personal information controller may notify third parties who have previously received such processed personal information. .

where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with	questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	

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?		

Accountability

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

Question	**Assessment Criteria**	**Enforceability** **(to be answered by the Economy)**
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. **· Internal guidelines or policies (if**	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	Section 7 of the Data Privacy Act of 2012 states that to administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the National Privacy Commission, winch shall have the following functions: 1. Ensure compliance of personal information controllers with the provisions of this Act; 2. Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any

applicable, describe how implemented) **· Contracts** **· Compliance with applicable industry or sector laws and regulations** **· Compliance with self-regulatory applicant code and/or rules** **Other (describe)**		such report: *Provided,* That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act; 3. Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest; 4. Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy; 5. Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act; 6. Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country; 7. Publish on a regular basis a guide to all laws relating to data protection; 8. Publish a compilation of agency system of records and notices, including index and other finding aids; 9. Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act; 10. Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers: *Provided,* That the privacy codes shall adhere to the underlying data privacy principles embodied in this Act: *Provided, further, t*hat such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the Commission shall consult with relevant regulatory agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons,

		entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law: *Provided, finally* that the Commission may review such privacy codes and require changes thereto for purposes of complying with this Act; 11. Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person; 12. Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws; 13. Propose legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary; 14. Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection; 15. Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws; 16. Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and 17. Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection. Section 21 of the law further states that each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

		1. The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. 2. The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles.	Section 21 of the law states that each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation: 1. The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.

	The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	2. The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/ Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal	Section 7 of the Data Privacy Act of 2012 states that the National Privacy Commission has the power to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided,* That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act. Furthermore, the Commission is also vested with power to recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of Data Privacy Act of 2012. The National Privacy Commission issued NPC Circular 16-04 which governs the rules of procedures in complaints lodged in the jurisdiction of the Commission.

	information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints.	Section 7 of the Data Privacy Act of 2012 states that the National Privacy Commission has the power to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided,* That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act. Furthermore, the Commission is also vested with power to recommend to the Department of Justice (DOJ) the prosecution and imposition of

	Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	penalties specified in Sections 25 to 29 of Data Privacy Act of 2012. The National Privacy Commission issued NPC Circular 16-04 which governs the rules of procedures in complaints lodged in the jurisdiction of the Commission.
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	Section 7 of the Data Privacy Act of 2012 states that the National Privacy Commission has the power to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided,* That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act. Furthermore, the Commission is also vested with power to recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of Data Privacy Act of 2012. The National Privacy Commission issued NPC Circular 16-04 which governs the rules of procedures in complaints lodged in the jurisdiction of the Commission.
44. Do you have procedures in	Where the Applicant answers **YES**, the Accountability Agent	Section 20 of the Data Privacy Act of 2012 states that the personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any

place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include: 1. Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability; 2. A security policy with respect to the processing of personal information; 3. A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and 4. Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach. The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures

		required by this provision. The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations. The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information. The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects. The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach. Also section 7 of the Data Privacy Act of 2012 states that the National Privacy Commission has the power to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided,* That in resolving any

		complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act. Furthermore, the Commission is also vested with power to recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of Data Privacy Act of 2012. The National Privacy Commission issued NPC Circular 16-04 which governs the rules of procedures in complaints lodged in the jurisdiction of the Commission.
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	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary	Section 12 of the law states that the processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: 1. The data subject has given his or her consent; 2. The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract; 3. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject; 4. The processing is necessary to protect vitally important interests of the data subject, including life and health;

personal information?	training to employees regarding this subject. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	5. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or 6. The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution. Section 13 of the law states that the processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: 1. The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing; 2. The processing of the same is provided for by existing laws and regulations: *Provided,* That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information; 3. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

		4. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided,* That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally,* That consent of the data subject was obtained prior to processing; 5. The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or 6. The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers	Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent	Section 14 of the law states that *a* personal information controller may subcontract the processing of personal information: *Provided,* That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.

pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? · Internal guidelines or policies _____ · Contracts _____ · Compliance with applicable industry or sector laws and regulations _____ · Compliance with self-regulatory applicant code and/or rules _____	must inform the Applicant that implementation of such agreements is required for compliance with this principle.	Section 44 of the IRR states that processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement. The contract or other legal act shall stipulate, in particular, that the personal information processor shall: 1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law; 2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data; 3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission; 4. Not engage another processor without prior instruction from the personal information controller: *Provided*, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing; 5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights; 6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor;

· Other (describe) _____		7. At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing: *Provided*, that this includes deleting existing copies unless storage is authorized by the Act or another law; 8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter; 9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission. Section 45 of the IRR states that the personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.
47. Do these agreements generally require that personal information	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	Section 14 of the law states that *a* personal information controller may subcontract the processing of personal information: *Provided,* That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information

processors, agents, contractors or other service providers: · Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement? _____ · Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____ · Follow instructions		processor shall comply with all the requirements of this Act and other applicable laws. Section 44 of the IRR states that processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement. The contract or other legal act shall stipulate, in particular, that the personal information processor shall: 1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law; 2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data; 3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission; 4. Not engage another processor without prior instruction from the personal information controller: *Provided*, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;

provided by you relating to the manner in which your personal information must be handled? _____ · Impose restrictions on subcontracting unless with your consent? _____ · Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____ · Notify the Applicant in the case of a breach of the personal information of		5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights; 6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor; 7. At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing: *Provided*, that this includes deleting existing copies unless storage is authorized by the Act or another law; 8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter; 9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission. Section 45 of the IRR states that the personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.

the Applicant's customers? . Other (describe)		
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.	The Accountability Agent must verify the existence of such self-assessments.	Section 44 states that the processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement. The contract or other legal act shall stipulate, in particular, that the personal information processor shall: 1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law; 2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data; 3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission; 4. Not engage another processor without prior instruction from the personal information controller: *Provided*, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing; 5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights; 6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission,

		taking into account the nature of processing and the information available to the personal information processor; 7. At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing: *Provided*, that this includes deleting existing copies unless storage is authorized by the Act or another law; 8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter; 9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission. Section 45 of the IRR states that the personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.
49. Do you carry out regular spot checking or monitoring of your personal	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures	Section 44 states that the processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the

information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	processing under the subcontracting agreement. The contract or other legal act shall stipulate, in particular, that the personal information processor shall: 1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law; 2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data; 3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission; 4. Not engage another processor without prior instruction from the personal information controller: *Provided*, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing; 5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights; 6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor; 7. At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing: *Provided*, that this includes deleting existing copies unless storage is authorized by the Act or another law;

		8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter; 9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission. Section 45 of the IRR states that the personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.
50. Do you disclose personal information to other recipient persons or organisations in situations where due diligence and reasonable steps to ensure compliance	If YES, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or	Section 14 of the law states that *a* personal information controller may subcontract the processing of personal information: *Provided,* That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws. Section 44 states that the processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information

with your APEC CBPRs by the recipient as described above is impractical or impossible?	impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	processor to the personal information controller. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement. The contract or other legal act shall stipulate, in particular, that the personal information processor shall: 1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law; 2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data; 3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission; 4. Not engage another processor without prior instruction from the personal information controller: *Provided*, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing; 5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights; 6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor; 7. At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the

		provision of services relating to the processing: *Provided*, that this includes deleting existing copies unless storage is authorized by the Act or another law; 8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter; 9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission. Section 45 of the IRR states that the personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.