

**CROSS-BORDER PRIVACY RULES SYSTEM
PARTICIPATION OF JAPAN**

**CROSS BORDER PRIVACY RULES SYSTEM JOINT OVERSIGHT PANEL
FINDINGS REPORT**

Submitted To: Ms. Lourdes Yapinchay
Chair, APEC Electronic Commerce Steering Group
Friday, 25 April 2014

TABLE OF CONTENTS

OVERVIEW AND PURPOSE	3
SUMMARY OF FINDINGS	4
FINDINGS OF THE JOINT OVERSIGHT PANEL	5
DISCUSSION OF FINDINGS	5
<i>Letter of Intent</i>	6
<i>Confirmation of CPEA Participation</i>	6
<i>Stated Intent to Make Use of APEC-Recognized Accountability Agent(s)</i>	7
<i>Relevant Laws, Regulations and Administrative Measures which may Apply to CBPR- Certification-Related Activities of an Accountability Agent Operating in Japan</i>	7
<i>APEC Cross Border Privacy Rules System Program Requirements Enforcement Map</i>	8
<i>Consultation Process</i>	8
SUSPENSION OR WITHDRAWAL OF PARTICIPATION	9
RE-INITIATION OF PARTICIPATION	9
APPENDIX	10
APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS: ENFORCEMENT MAP	10

OVERVIEW AND PURPOSE

The purpose of this findings report is to assess Japan's application to formally participate in the APEC Cross Border Privacy Rules system. Paragraph 6.2 of the Charter of the APEC Cross Border Privacy Rules Joint Oversight Panel (herein "Charter") identifies the core functions of the Joint Oversight Panel (herein "JOP") and instructs the JOP to "[e]ngage in consultations with those Economies that have indicated an intention to participate in the Cross Border Privacy Rules (herein "CBPR") System and issue a report as to how the conditions set out in paragraph 2.2 have been met." This report details how the conditions in paragraph 2.2 have been met.

Conditions set out in paragraph 2.2 of the Charter require that the following be submitted to the Chair of the Electronic Commerce Steering Group (herein "ECSG"), the Chair of the Data Privacy Subgroup (herein "DPS") and the Chair of the JOP:

- A letter of intent to participate in the CBPR System;
- Confirmation that a Privacy Enforcement Authority in that Economy is a participant in the Cross Border Privacy Enforcement Arrangement (herein "CPEA");
- Confirmation that the Economy intends to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2 of the Charter (*note: the Economy need not name a specific Accountability Agent at this point, only affirm its intention to use the services of an APEC-recognized Accountability Agent once it has been identified and approved*);
- With respect to Accountability Agents, a narrative description of the relevant domestic laws and regulations and administrative measures which may apply to any CBPR System certification-related activities of an Accountability Agent operating within the Economy's jurisdiction and the enforcement authority associated with these laws and regulations and administrative measures; and
- The Completed APEC Cross-Border Privacy Rules System Program Requirements Enforcement Map and additional narrative explanation of the Economy's ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR System program requirements.

Following is a findings report that details the consultative process undertaken with the relevant government representatives from Japan and an explanation of how each of the conditions set out in paragraph 2.2 of the Charter has been met.

This report is to be circulated to all member Economies by the APEC Secretariat and made publicly available on the APEC website as well as the CBPR System website.

SUMMARY OF FINDINGS

In a letter dated 7 June 2013, Japan's APEC Senior Officials from the Ministry of Foreign Affairs and the Ministry of Economy, Trade and Industry (herein "METI") provided the Chair of the APEC ECSG Japan's *Notice of Intent to Participate in the CBPR System*. The letter contained confirmation of the following:

- 1) The Cabinet Office; Consumer Affairs Agency; Financial Services Agency; the National Police Agency; Ministry of Internal Affairs and Communications; Ministry of Justice; Ministry of Foreign Affairs; Ministry of Finance; Ministry of Education, Culture, Sports, Science and Technology; Ministry of Health, Labour and Welfare; Ministry of Agriculture, Forestry and Fisheries; Ministry of Economy, Trade and Industry; Ministry of Land, Infrastructure, Transport and Tourism; Ministry of Environment; and Ministry of Defense, are participants in the Cross Border Privacy Enforcement Arrangement (CPEA); and
- 2) Japan intends to have at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2 of the Charter.

Appended to this Notice of Intent, under Annex A and Annex B respectively, were the following documents:

- 1) A narrative description of the relevant domestic laws and regulations that may apply to any CBPR certification-related activities of an Accountability Agent operating within Japan and the enforcement authority associated with these laws and regulations; and
- 2) The completed APEC CBPR System Program Requirements Enforcement Map.

FINDINGS OF THE JOINT OVERSIGHT PANEL

Having verified the completeness of Japan's Notice of Intent to Participate;

Having consulted with representatives from the Ministry of the Economy, Trade and Industry and the Consumer Affairs Agency of Japan on the narrative description of domestic laws and regulations applicable to the certification-related activities of Accountability Agents operating in Japan, and on the completed APEC Cross-Border Privacy Rules System Program Requirements Enforcement Map;

Having verified with the Administrators of the APEC Cross Border Privacy Enforcement Arrangement (CPEA) that the Cabinet Office; Consumer Affairs Agency; Financial Services Agency; the National Police Agency; Ministry of Internal Affairs and Communications; Ministry of Justice; Ministry of Foreign Affairs; Ministry of Finance; Ministry of Education, Culture, Sports, Science and Technology; Ministry of Health, Labour and Welfare; Ministry of Agriculture, Forestry and Fisheries; Ministry of Economy, Trade and Industry; Ministry of Land, Infrastructure, Transport and Tourism; Ministry of Environment; and Ministry of Defense, are participants in the APEC CPEA;

The Cross Border Privacy Rules System Joint Oversight Panel finds that the conditions established in paragraph 2.2 (i-iii) of the Charter, establishing the requirements for recognition as a Participant in the Cross Border Privacy Rules System, have been met by Japan.


The Cross Border Privacy Rules Joint Oversight Panel invites the Chair of the APEC ECSG to notify Japan that the conditions set out in Paragraph 2.2 of the Charter have been met, and to advise them that they are hereby considered a Participant in the CBPR System.

Once the notification has been given by the Chair of the ECSG, Japan may nominate one or more Accountability Agents for APEC recognition or notify the JOP of a request by the Accountability Agent(s), for recognition under the CBPR System.

Signed,



Daniele Chatelois
Chair, Joint Oversight Panel (designee)
Industry Canada



Colin Minihan
Co-Chair, Joint Oversight Panel
Attorney General's Department, Australia



Elizabeth Argüello Maya
Co-Chair, Joint Oversight Panel
Ministry of Economy, Mexico

DISCUSSION OF FINDINGS

Letter of Intent

On 7 June 2013, the Chair of the APEC ECSG received a letter from Japan's APEC Senior Officials from the Ministry of Foreign Affairs and METI, indicating Japan's intent to participate in the APEC Cross Border Privacy Rules (herein "CBPR") System. The letter makes the following statements:

- 1) The Cabinet Office; Consumer Affairs Agency; Financial Services Agency; the National Police Agency; Ministry of Internal Affairs and Communications; Ministry of Justice; Ministry of Foreign Affairs; Ministry of Finance; Ministry of Education, Culture, Sports, Science and Technology; Ministry of Health, Labour and Welfare; Ministry of Agriculture, Forestry and Fisheries; Ministry of Economy, Trade and Industry; Ministry of Land, Infrastructure, Transport and Tourism; Ministry of Environment; and Ministry of Defense, are participants in the Cross Border Privacy Enforcement Arrangement (CPEA);
- 2) Japan intends to have at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2 of the Charter.

Appended to the letter, under Annex A and Annex B respectively, were the following documents:

- 1) A narrative description of the relevant Japanese laws and regulations that may apply to any CBPR certification-related activities of an Accountability Agent operating within Japan's jurisdiction and the enforcement authority associated with these laws and regulations.
- 2) The APEC CBPR System Program Requirements Enforcement Map, completed by Japan, outlining the identified enforcement authorities' ability to take enforcement actions under applicable laws and regulations that have the effect of protecting personal information consistently with the CBPR System program requirements.

Confirmation of CPEA Participation

In its 7 June 2013 *Notice of Intent to Participate* in the APEC CBPR System, Japan confirmed that: the Cabinet Office; Consumer Affairs Agency; Financial Services Agency; the National Police Agency; Ministry of Internal Affairs and Communications; Ministry of Justice; Ministry of Foreign Affairs; Ministry of Finance; Ministry of Education, Culture, Sports, Science and Technology; Ministry of Health, Labour and Welfare; Ministry of Agriculture, Forestry and Fisheries; Ministry of Economy, Trade and Industry; Ministry of Land, Infrastructure, Transport and Tourism; Ministry of Environment; and Ministry of Defense, are participants in the Cross Border Privacy Enforcement Arrangement (CPEA).

On 5 February 2014 the JOP obtained written confirmation of the participation these Privacy Enforcement Authorities (PEAs) from the Framework Administrators of the APEC CPEA. The

letter is attached to this report. Current CPEA membership can be found at:

<http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>

Based on consultations with METI and the Consumer Affairs Agency, and confirmation by the CPEA Administrators, the JOP finds that Japan meets the corresponding requirement for Member Economy participation, as set out in paragraph 2.2 of the Charter.

Stated Intent to Make Use of APEC-Recognized Accountability Agent(s)

Japan's *Notice of Intent to Participate* includes a confirmation that Japan expects to have at least one APEC-recognized Accountability Agent, subject to the procedures outlined in paragraph 6.2 of the Charter. The JOP finds that this confirmation by the Ministry of Foreign Affairs and METI meets the corresponding requirement for Member Economy participation, as set out in paragraph 2.2 of the Charter.

Relevant Laws, Regulations and Administrative Measures which may Apply to CBPR-Certification-Related Activities of an Accountability Agent Operating in Japan

Annex A of Japan's *Notice of Intent to Participate* outlines the laws, regulations and administrative measures which may apply to the CBPR certification-related activities of an Accountability Agent operating within Japan. Annex A also details the enforcement authority associated with these laws, regulations and administrative measures.

Under Article 46 of Japan's *Act on the Protection of Personal Information*, a competent Minister may require an authorized personal information protection organization ("Accountability Agent") make a report regarding its privacy-certification related practices. Additionally, under Article 47, a competent Minister may order the Accountability Agent to "improve its methods of conducting its authorized businesses, amend its personal information protection guidelines, or to take any other necessary measures to the extent necessary for implementation of the provisions of this section." Should an Accountability Agent fails to obey this order, a competent Minister may rescind the authorization of that Accountability Agent to operate in Japan pursuant to Article 48(1). In this case, the Accountability Agent is prohibited from any certification-related activities as part of the CBPR system. Through this authority, Japan may nominate and submit to the ECSG, the DPS and the JOP, the relevant application and associated documentation of those accredited certifiers seeking APEC recognition as an Accountability Agent in the APEC CBPR System.

APEC Cross Border Privacy Rules System Program Requirements Enforcement Map

Annex B of Japan's *Notice of Intent to Participate* contains the completed APEC Cross- Border Privacy Rules System Program Requirements Enforcement Map. In this Map, Japan provided citations to all relevant provisions in the *Act on the Protection of Personal Information (herein 'Act')*, the *Cabinet Order for the Enforcement of the Act on the Protection of Personal Information (herein 'Cabinet Order')*, and the *Basic Policy on the Protection of Personal Information (herein 'Basic Policy')*, that have the effect of protecting personal information consistent with the CBPR System program requirements¹.

The Joint Oversight Panel reviewed the Japan submission to verify the applicability of each cited Article of the Law and/or Regulation, including the Cabinet Order and the Basic Policy, to the relevant program requirement (*see Appendix*).

Consultation Process

As instructed in the Charter and in the JOP Protocols document, the JOP engaged in consultations with relevant parties in preparation for the submission of this report to the Chair of the ECSG. The purpose of these consultations was to obtain further details and clarifications on certain elements of Japan's *Notice of Intent to Participate* in the CBPR System, including information provided in Annex A and Annex B, and to obtain confirmation of the identified Privacy Enforcement Authorities' participation in the CPEA. Consultations were undertaken with representatives of METI, the Consumer Affairs Agency and Administrators of the CPEA. These consultations took place via email, teleconference and in-person in Tokyo, Japan as well as in Ningbo, China during SOM1 2014 meetings.

¹ The Act, Cabinet Order and Basic Policy can be accessed at the following URLs:

Act on the Protection of Personal Information
<http://www.caa.go.jp/seikatsu/kojin/foreign/act.pdf>

Cabinet Order for the Enforcement of the Act on the Protection of Personal Information
<http://www.caa.go.jp/seikatsu/kojin/foreign/cabinet-order.pdf>

Basic Policy on the Protection of Personal Information
<http://www.caa.go.jp/seikatsu/kojin/foreign/basic-policy-tentver.pdf>

SUSPENSION OR WITHDRAWAL OF PARTICIPATION

Participation by Japan in the CBPR System may be suspended by a consensus determination by all APEC member Economies (excluding both the requesting Economy and the Economy in question) that one or more of the following situations has occurred:

- Revocation, repeal or amendment of any domestic laws and/or regulations having the effect of making participation in the CBPR system impossible (such as repeal of a law that has the effect of protecting personal information consistent with the CBPR program requirements);
- The CBPR Participant's Privacy Enforcement Authority as defined in paragraph 4.1 of the CPEA ceases participation pursuant to paragraph 8.2 of the CPEA; or
- Dissolution or disqualification of a previously recognized Accountability Agent where this function is provided in the CBPR Participant's Economy exclusively by that entity (*note: certification of those organizations only certified by that Accountability Agent will be terminated until such time as the Economy is able to again fulfill the requirement for participation in the CBPR System pursuant to the process described in paragraphs 1-5 in the Protocols of the Joint Oversight Panel, at which time any previously-certified applicant organizations should complete a new certification process. However, existing legal obligations may remain in effect under domestic law.*)

Only CBPR Participating Economies may initiate a request for a consensus determination that any situation identified above has occurred.

Japan may cease participation in the CBPR System at any time by giving 30 days' written notice (beginning from the date the notice is received) to the ECSG Chair.

If Japan ceases participation (whether by way of withdrawal or suspension) in the CBPR System, any certifications performed by APEC-recognized Accountability Agents operating in Japan must be suspended at the same time as the cessation of the Economy's participation in the CBPR System. This requirement must be incorporated into the agreements between the Accountability Agents and any organizations they certify as CBPR-compliant. However, existing legal obligations may remain in effect under domestic law.

RE-INITIATION OF PARTICIPATION

Any APEC member Economy that has withdrawn or is suspended from participation in the CBPR System may engage in consultations with the JOP to re-initiate participation pursuant to the process described in paragraphs 1-5 of the Protocols of the Joint Oversight Panel at any time.

APPENDIX

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

The purpose of this Appendix is to identify all relevant provisions in the Act on the Protection of Personal Information (herein ‘Act’), the Cabinet Order for the Enforcement of the Act on the Protection of Personal Information (herein ‘Cabinet Order’), and the Basic Policy on the Protection of Personal Information (herein ‘Basic Policy’)², relevant to the enforceability of each of the 50 CBPR program requirements. This summary only provides the relevant text of clauses within those identified provisions necessary for the enforcement of each of the CBPR program requirements and is not intended to represent all obligations and rights provided under Japanese law.

NOTICE

COLLECTION LIMITATION

USES OF PERSONAL INFORMATION

CHOICE.....

INTEGRITY OF PERSONAL INFORMATION.....

SECURITY SAFEGUARDS

ACCESS AND CORRECTION.....

ACCOUNTABILITY.....

2

Note: The Scope of the Act is stipulated in Article 1 (Purpose) of the Act. Obligations on business organizations are stipulated in Articles 15 to 31 of the Act.

As stipulated in the chapeau paragraph of the Cabinet Order, the Cabinet Order provides details on relevant Articles of the Act. Accordingly, the Cabinet Order requires applies to business organizations in line with the Act.

As stipulated in the chapeau paragraph of the Cabinet Decision (Basic Policy), the Basic Policy is established based on Article 7 of the Act, and in line with the purpose stipulated in Article 1 of the Act. As stipulated in Article 7 (2)(6) of the Act, the Cabinet Decision (Basic Policy) establishes obligations to be followed by business organizations for the protection of personal information. Accordingly, business organizations are required to follow the Cabinet Decision (Basic Policy) in line with the Act.

Enforcement of the Act by the minister in charge (Competent Minister) is exercised according to Article 32 to Article 35 of the Act. When the Competent Minister finds that a business organization is not fulfilling the requirements as stipulated in the Act or the Cabinet Order, or the Cabinet Decision (Basic Policy), the Competent Minister will take necessary measures in accordance with Article 32 to Article 35 of the Act.

NOTICE

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

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	JOP Finding
<p>1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)?</p> <p>Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.</p>	<p>If YES, the Accountability Agent must verify that the Applicant’s privacy practices and policy (or other privacy statement) include the following characteristics:</p> <ul style="list-style-type: none"> • Available on the Applicant’s Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible; • Applies to all personal information; whether collected online or offline; • States an effective date of Privacy Statement publication. <p>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.</p>	<p>ACT</p> <p>Article 18 (1) When having acquired personal information, a business operator handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of Utilization.</p> <p>Article 24 (1): With respect to the retained personal data, a business operator handling personal information shall put the matters listed in the following items in an accessible condition for the person (such condition includes cases in which a response is made without delay at the request of the person):</p> <ol style="list-style-type: none"> i. The name of the business operator handling personal information ii. The Purpose of Utilization of all retained personal data (except in cases falling under any of items (i) to (iii) of paragraph (4) of Article 18) iii. Procedures to meet requests made pursuant to the provisions of the next paragraph, paragraph (1) of the next article, paragraph (1) of Article 26, or paragraph (1) or paragraph (2) of Article 27

	<p>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>(including the amount of charges if set pursuant to the provision of paragraph (2) of Article 30)</p> <p>iv. In addition to what is listed in the preceding three items, such matters, specified by a Cabinet Order, as being necessary for ensuring the proper handling of retained personal data</p> <p><i>BASIC POLICY</i></p> <p>Article 6(1)a: To maintain the society’s trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy to understand manner, their procedures related to the handling of personal information, such as notification and announcement of the purpose of use and disclosure etc., as well as comply with the relevant laws and ordinances.</p>
<p>1.a) Does this privacy statement describe how personal information is collected?</p>	<p>If YES, the Accountability Agent must verify that:</p> <ul style="list-style-type: none"> • The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. • The Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and 	<p><i>ACT</i></p> <p>Article 17 A business operator handling personal information shall not acquire personal information by a deception or other wrongful means.</p> <p><i>BASIC POLICY</i></p> <p>Article 6(1)b: From the viewpoint of the protection of the rights and interests of the concerned persons, it is important</p>

	<ul style="list-style-type: none"> • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. <p>If NO, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.</p>	<p>to further improve response to the requests of concerned persons, such as consumers etc., in the policies and philosophies on the promotion of personal information protection...by including statements that consider the following points:</p> <ul style="list-style-type: none"> • Whether information is entrusted to others or not, promoting the clarification of outside processing, such as clarifying the details of work done outside the business by outsourcers. • Specifying as concretely as possible the source the personal information was acquired from and the method of acquisition (the type of acquisition source etc.)
<p>1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the applicant provides notice to individuals of the purpose for which personal information is being collected.</p> <p>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.</p>	<p><i>ACT</i></p> <p>Article 18 (1) When having acquired personal information, a business operator handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of Utilization.</p> <p><i>BASIC POLICY</i></p> <p>Article 6(1)a: To maintain the society’s trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy to understand manner, their procedures related to the handling of personal</p>

		<p>information, such as notification and announcement of the purpose of use and disclosure etc., as well as comply with the relevant laws and ordinances.</p>
<p>1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?</p>	<p>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.</p> <p>Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement.</p> <p>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>ACT</p> <p>Article 23</p> <p>(1): A business operator handling personal information shall not, except in the following cases, provide personal data to a third party without obtaining the prior consent of the person:</p> <ul style="list-style-type: none"> (i) Cases in which the provision of personal data is based on laws and regulations (ii) Cases in which the provision of personal data is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person (iii) Cases in which the provision of personal data is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person (iv) Cases in which the provision of personal data is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by one in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person are likely to impede the execution of the Affairs <p>(2) With respect to personal data intended to be provided to a third party, where a business operator handling personal information agrees to discontinue, at the request of a person, the provision of such personal data as will lead to the identification of the person, and where the business operator, in advance, notifies the person of the matters listed in the following items or put those matters</p>

		<p>in a readily accessible condition for the person, the business operator may, notwithstanding the provision of the preceding paragraph, provide such personal data to a third party:</p> <ul style="list-style-type: none">(i) The fact that the provision to a third party is the Purpose of Utilization(ii) The items of the personal data to be provided to a third party(iii) The means or method of provision to a third party(iv) The fact that the provision of such personal data as will lead to the identification of the person to a third party will be discontinued at the request of the person <p>(3) When a business operator handling personal information changes the matter listed in item (ii) or (iii) of the preceding paragraph, the business operator shall, in advance, notify the person of the content of the change or put it in a readily accessible condition for the person.</p> <p>(4) In following the cases, the individual or business operator receiving such personal data shall not be deemed a third party for the purpose of application of the provisions of the preceding three paragraphs:</p> <ul style="list-style-type: none">(i) Cases in which a business operator handling personal information entrust the handling of personal data in whole or in part within the scope necessary for the achievement of the Purpose of Utilization(ii) Cases in which personal data is provided as a result of the succession of business in a merger or otherwise(iii) Cases in which personal data is used jointly between specific individuals or entities and in which this fact, the items of the personal data used jointly, the scope of the joint users, the purpose for which the personal data is used by them, and the name of the individual or business operator responsible for the management of the personal data is, in advance, notified to the person
--	--	--

		<p>or put in a readily accessible condition for the person</p> <p>(5) When a business operator handling personal information changes the purpose for which the personal data is used or the name of the individual or business operator responsible for the management of the personal data as are provided in item (iii) of the preceding paragraph, the business operator shall, in advance, notify the person of the content of the change or put it in a readily accessible condition for the person.</p> <p>BASIC POLICY</p> <p>Article 6(1)b: From the viewpoint of the protection of the rights and interests of the concerned persons, it is important to further improve response to the requests of concerned persons, such as consumers etc., in the policies and philosophies on the promotion of personal information protection...by including statements that consider the following points:...</p> <ul style="list-style-type: none"> • Whether information is entrusted to others or not, promoting the clarification of outside processing, such as clarifying the details of work done outside the business by outsourcers. • Specifying as concretely as possible the source the personal information was acquired from and the method of acquisition (the type of acquisition source etc.)
<p>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</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides name, address and a functional e-mail address.</p> <p>Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant</p>	<p>ACT</p> <p>Article 24</p> <p>(1): With respect to the retained personal data, a business operator handling personal information shall put the matters listed in the following items in an accessible condition for the person (such condition includes cases in which a response is made without delay at the request of</p>

<p>collection?</p> <p>Where YES describe.</p>	<p>that such disclosure of information is required for compliance with this principle.</p> <p>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>the person):</p> <ul style="list-style-type: none"> (i) The name of the business operator handling personal information (ii) The Purpose of Utilization of all retained personal data (except in cases falling under any of items (i) to (iii) of paragraph (4) of Article 18) (iii) Procedures to meet requests made pursuant to the provisions of the next paragraph, paragraph (1) of the next article, paragraph (1) of Article 26, or paragraph (1) or paragraph (2) of Article 27 (including the amount of charges if set pursuant to the provision of paragraph (2) of Article 30) (iv) In addition to what is listed in the preceding three items, such matters, specified by a Cabinet Order, as being necessary for ensuring the proper handling of retained personal data <p>CABINET ORDER</p> <p>Article 5 Matters specified by a Cabinet Order under Item 4 of Paragraph 1 of Article 24 of the Act shall be the matters as set forth below:</p> <ul style="list-style-type: none"> (1) The place where a complaint concerning the handling of retained personal data by the entity handling personal information concerned is lodged. (2) If the entity handling personal information concerned is a target entity of an authorized personal information protection organization, the name of the authorized personal information protection organization concerned and the place where settlement of the complaint is lodged.
<p>1.e) Does this privacy statement provide</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the</p>	<p>ACT</p>

<p>information regarding the use and disclosure of an individual's personal information?</p>	<p>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.</p> <p>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.</p> <p>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>Article 18 (1)When having acquired personal information, a business operator handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of Utilization.</p> <p>BASIC POLICY</p> <p>Article 6(1)b: From the viewpoint of the protection of the rights and interests of the concerned persons, it is important to further improve response to the requests of concerned persons, such as consumers etc., in the policies and philosophies on the promotion of personal information protection...by including statements that consider the following points:...</p> <ul style="list-style-type: none"> • Whether information is entrusted to others or not, promoting the clarification of outside processing, such as clarifying the details of work done outside the business by outsourcers. • Specifying as concretely as possible the source the personal information was acquired from and the method of acquisition (the type of acquisition source etc.)
<p>1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Privacy Statement includes:</p> <ul style="list-style-type: none"> • 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 	<p>ACT</p> <p>Article 24 (1) With respect to the retained personal data, an entity handling personal information, must put the matters enumerated in the following items in an accessible condition for the person... (iii) Procedures to meet requests made pursuant to the</p>

	<p>order to correct his or her personal information.</p> <p>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.</p> <p>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>provisions...of paragraph 1 or Article 26.</p> <p>Article 26 (1) When a business operator handling personal information is requested by a person to correct, add, or delete such retained personal data as may lead to the identification of the person on the ground that the retained personal data is contrary to the fact, the business operator shall, except in cases in which special procedures are prescribed by any other laws and regulations for such correction, addition, or deletion, make a necessary investigation without delay within the scope necessary for the achievement of the Purpose of Utilization and, on the basis of the results, correct, add, or delete the retained personal data.</p> <p>Article 29 (1) A business operator handling personal information may, as prescribed by a Cabinet Order, determine procedures for receiving requests that may be made pursuant to the provisions of paragraph (2) of Article 24, paragraph (1) of Article 25, paragraph (1) of Article 26 or paragraph (1) or paragraph (2) of Article 27 (hereinafter referred to as "a request for disclosure and others" in this article). In such a case, any person making a request for disclosure and others shall comply with the procedures.</p>
<p>2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals.</p> <p>Where the Applicant answers NO and does not identify an applicable qualification, the</p>	<p><i>ACT</i></p> <p>Article 18 (1)When having acquired personal information, a business operator handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of</p>

<p>information is being collected?</p>	<p>Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle.</p> <p>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>Utilization.</p> <p>(2)Notwithstanding the provision of the preceding paragraph, when a business operator handling personal information acquires such personal information on a person as is written in a contract or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. hereinafter the same shall apply in this paragraph.) as a result of concluding a contract with the person or acquires such personal information on a person as is written in a document directly from the person, the business operator shall expressly show the Purpose of Utilization in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.</p> <p>(3)When a business operator handling personal information has changed the Purpose of Utilization, the business operator shall notify the person of the changed Purpose of Utilization or publicly announce it.</p> <p>(4)The provisions of the preceding three paragraphs shall not apply to the following cases:</p> <ul style="list-style-type: none">(i) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the life, body, property, or other rights or interests of the person or a third party(ii) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the rights or legitimate interests of the business operator handling personal information(iii) Cases in which it is necessary to cooperate with a state organ or a local government in executing the affairs prescribed by laws and regulations and in
--	---	---

		<p>which notifying the person of the Purpose of Utilization or publicly announcing it are likely to impede the execution of the affairs</p> <p>(iv) Cases in which it is considered that the Purpose of Utilization is clear in consideration of the circumstances of the acquisition</p>
<p>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?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other.</p> <p>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.</p> <p>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p><i>ACT</i></p> <p>Article 18</p> <p>(1)When having acquired personal information, a business operator handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of Utilization.</p> <p>(2)Notwithstanding the provision of the preceding paragraph, when a business operator handling personal information acquires such personal information on a person as is written in a contract or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. hereinafter the same shall apply in this paragraph.) as a result of concluding a contract with the person or acquires such personal information on a person as is written in a document directly from the person, the business operator shall expressly show the Purpose of Utilization in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.</p> <p>(3)When a business operator handling personal information has changed the Purpose of Utilization, the business operator shall notify the person of the changed Purpose of Utilization or publicly announce it.</p>

		<p>(4)The provisions of the preceding three paragraphs shall not apply to the following cases:</p> <ul style="list-style-type: none"> (i) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the life, body, property, or other rights or interests of the person or a third party (ii) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the rights or legitimate interests of the business operator handling personal information (iii) Cases in which it is necessary to cooperate with a state organ or a local government in executing the affairs prescribed by laws and regulations and in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to impede the execution of the affairs (iv) Cases in which it is considered that the Purpose of Utilization is clear in consideration of the circumstances of the acquisition
<p>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?</p>	<p>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.</p> <p>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.</p> <p>Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is</p>	<p><i>ACT</i></p> <p>Article 18</p> <p>(1)When having acquired personal information, a business operator handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of Utilization.</p> <p>(2)Notwithstanding the provision of the preceding paragraph, when a business operator handling personal information acquires such personal information on a person as is written in a contract or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable</p>

	<p>justified.</p>	<p>to human senses. hereinafter the same shall apply in this paragraph.) as a result of concluding a contract with the person or acquires such personal information on a person as is written in a document directly from the person, the business operator shall expressly show the Purpose of Utilization in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.</p> <p>(3)When a business operator handling personal information has changed the Purpose of Utilization, the business operator shall notify the person of the changed Purpose of Utilization or publicly announce it.</p> <p>(4)The provisions of the preceding three paragraphs shall not apply to the following cases:</p> <ul style="list-style-type: none">(i) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the life, body, property, or other rights or interests of the person or a third party(ii) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the rights or legitimate interests of the business operator handling personal information(iii) Cases in which it is necessary to cooperate with a state organ or a local government in executing the affairs prescribed by laws and regulations and in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to impede the execution of the affairs <p>Cases in which it is considered that the Purpose of Utilization is clear in consideration of the circumstances of the acquisition</p>
--	-------------------	--

		<p>Article 23</p> <p>(1) A business operator handling personal information shall not, except in the following cases, provide personal data to a third party without obtaining the prior consent of the person:</p> <ul style="list-style-type: none">(i) Cases in which the provision of personal data is based on laws and regulations(ii) Cases in which the provision of personal data is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person(iii) Cases in which the provision of personal data is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person(iv) Cases in which the provision of personal data is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by one in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person are likely to impede the execution of the affairs <p>(2) With respect to personal data intended to be provided to a third party, where a business operator handling personal information agrees to discontinue, at the request of a person, the provision of such personal data as will lead to the identification of the person, and where the business operator, in advance, notifies the person of the matters listed in the following items or put those matters in a readily accessible condition for the person, the business operator may, notwithstanding the provision of the preceding paragraph, provide such personal data to a third party:</p> <ul style="list-style-type: none">(i) The fact that the provision to a third party is the Purpose of Utilization(ii) The items of the personal data to be provided to a third party
--	--	---

		<p>(iii) The means or method of provision to a third party</p> <p>(iv) The fact that the provision of such personal data as will lead to the identification of the person to a third party will be discontinued at the request of the person</p> <p>(4) In following the cases, the individual or business operator receiving such personal data shall not be deemed a third party for the purpose of application of the provisions of the preceding three paragraphs:</p> <p>(i) Cases in which a business operator handling personal information entrust the handling of personal data in whole or in part within the scope necessary for the achievement of the Purpose of Utilization</p> <p>(ii) Cases in which personal data is provided as a result of the succession of business in a merger or otherwise</p> <p>(iii) Cases in which personal data is used jointly between specific individuals or entities and in which this fact, the items of the personal data used jointly, the scope of the joint users, the purpose for which the personal data is used by them, and the name of the individual or business operator responsible for the management of the personal data is, in advance, notified to the person or put in a readily accessible condition for the person.</p> <p><i>BASIC POLICY</i></p> <p>Article 6(1)b: From the viewpoint of the protection of the rights and interests of the concerned persons, it is important to further improve response to the requests of concerned persons, such as consumers etc., in the policies and philosophies on the promotion of personal information protection...by including statements that consider the following points:</p> <ul style="list-style-type: none">• Whether information is entrusted to others or not,
--	--	---

		<p>promoting the clarification of outside processing, such as clarifying the details of work done outside the business by outsourcers.</p> <ul style="list-style-type: none">• Specifying as concretely as possible the source the personal information was acquired from and the method of acquisition (the type of acquisition source etc.)
--	--	---

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)	JOP Finding
<p>5. How do you obtain personal information:</p> <p>5.a) Directly from the individual?</p> <p>5.b) From third parties collecting on your behalf?</p> <p>5.c) Other. If YES, describe.</p>	<p>The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information.</p> <p>Where the Applicant answers YES to any of these sub- parts, the Accountability Agent must verify the Applicant’s practices in this regard.</p> <p>There should be at least one ‘yes’ answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.</p>	<p>ACT</p> <p>Article 17</p> <p>A business operator handling personal information shall not acquire personal information by a deception or other wrongful means.</p> <p>BASIC POLICY</p> <p>Article 6(1)b: From the viewpoint of the protection of the rights and interests of the concerned persons, it is important to further improve response to the requests of concerned persons, such as consumers etc., in the policies and philosophies on the promotion of personal information protection...by including statements that consider the following points:...</p> <ul style="list-style-type: none"> • Whether information is entrusted to others or not, promoting the clarification of outside processing, such as clarifying the details of work done outside the business by outsourcers. • Specifying as concretely as possible the source the personal information was acquired from and the method of acquisition (the type of acquisition source etc.)
<p>6. Do you limit your personal information collection (whether</p>	<p>Where the Applicant answers YES and indicates it only collects personal information which is relevant to the identified collection purpose or other</p>	<p>ACT</p>

<p>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?</p>	<p>compatible or related purposes, the Accountability Agent must require the Applicant to identify:</p> <ul style="list-style-type: none"> • Each type of data collected; • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data; • An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection. <p>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.</p> <p>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.</p>	<p>Article 16</p> <p>(1) A business operator handling personal information shall not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Utilization specified pursuant to the provision of the preceding article.</p>
<p>7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information?</p> <p>Where YES, describe.</p>	<p>Where the Applicant answers YES, the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception.</p> <p>Where the Applicant Answers NO, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.</p>	<p>ACT</p> <p>Article 17</p> <p>A business operator handling personal information shall not acquire personal information by a deception or other wrongful means.</p>

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)	JOP Finding
<p>8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes.</p> <p>Where the Applicant Answers NO, the Accountability Agent must consider answers to Question 9 below.</p>	<p>ACT</p> <p>Article 16 (1) A business operator handling personal information shall not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Utilization specified pursuant to the provision of the preceding article.</p>
<p>9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following</p>	<p>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.</p>	<p>ACT</p> <p>Article 16 (1) A business operator handling personal information shall not handle personal information about a person,</p>

<p>circumstances?</p> <p>Describe below.</p> <p>9.a) Based on express consent of the individual?</p> <p>9.b) Compelled by applicable laws?</p>	<p>Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant’s use of the personal information is based on express consent of the individual (9.a), such as:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below.</p> <p>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.</p> <p>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</p>	<p>without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Utilization specified pursuant to the provision of the preceding article.</p> <p>(3) The provisions of the preceding two paragraphs shall not apply to the following cases:</p> <ul style="list-style-type: none"> (i) Cases in which the handling of personal information is based on laws and regulations (ii) Cases in which the handling of personal information is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person (iii) Cases in which the handling of personal information is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person (iv) Cases in which the handling of personal information is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by either of the former two in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person is likely to impede the execution of the affairs concerned
--	--	--

	<p>collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.</p>	
<p>10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers?</p> <p>If YES, describe.</p>	<p>Where the Applicant answers YES in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law.</p> <p>Also, the Accountability Agent must require the Applicant to identify:</p> <ol style="list-style-type: none"> 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes. 	<p>ACT</p> <p>Article 23</p> <p>(1) A business operator handling personal information shall not, except in the following cases, provide personal data to a third party without obtaining the prior consent of the person:</p> <ol style="list-style-type: none"> (i) Cases in which the provision of personal data is based on laws and regulations (ii) Cases in which the provision of personal data is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person (iii) Cases in which the provision of personal data is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person (iv) Cases in which the provision of personal data is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by one in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person are likely to impede the execution of the affairs <p>(2) With respect to personal data intended to be provided to a third party, where a business operator handling personal information agrees to discontinue, at the request of a person, the provision of such personal data as will lead to the identification of the person, and where the business operator, in advance, notifies the person of the matters</p>

		<p>listed in the following items or put those matters in a readily accessible condition for the person, the business operator may, notwithstanding the provision of the preceding paragraph, provide such personal data to a third party:</p> <ul style="list-style-type: none"> (i) The fact that the provision to a third party is the Purpose of Utilization (ii) The items of the personal data to be provided to a third party (iii) The means or method of provision to a third party (iv) The fact that the provision of such personal data as will lead to the identification of the person to a third party will be discontinued at the request of the person <p>(4) In following the cases, the individual or business operator receiving such personal data shall not be deemed a third party for the purpose of application of the provisions of the preceding three paragraphs:</p> <ul style="list-style-type: none"> (i) Cases in which a business operator handling personal information entrust the handling of personal data in whole or in part within the scope necessary for the achievement of the Purpose of Utilization (ii) Cases in which personal data is provided as a result of the succession of business in a merger or otherwise (iii) Cases in which personal data is used jointly between specific individuals or entities and in which this fact, the items of the personal data used jointly, the scope of the joint users, the purpose for which the personal data is used by them, and the name of the individual or business operator responsible for the management of the personal data is, in advance, notified to the person or put in a readily accessible condition for the person.
<p>11. Do you transfer personal information to personal information</p>		<p><i>ACT</i></p> <p>Article 23</p>

<p>processors? If YES, describe.</p>		<p>(1) A business operator handling personal information shall not, except in the following cases, provide personal data to a third party without obtaining the prior consent of the person: Cases in which the provision of personal data is based on laws and regulations</p> <ul style="list-style-type: none">(i) Cases in which the provision of personal data is based on laws and regulations(ii) Cases in which the provision of personal data is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person(iii) Cases in which the provision of personal data is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person(iv) Cases in which the provision of personal data is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by one in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person are likely to impede the execution of the affairs <p>(2) With respect to personal data intended to be provided to a third party, where a business operator handling personal information agrees to discontinue, at the request of a person, the provision of such personal data as will lead to the identification of the person, and where the business operator, in advance, notifies the person of the matters listed in the following items or put those matters in a readily accessible condition for the person, the business operator may, notwithstanding the provision of the preceding paragraph, provide such personal data to a third party:</p> <ul style="list-style-type: none">(i) The fact that the provision to a third party is the Purpose of Utilization(ii) The items of the personal data to be provided to a
--------------------------------------	--	--

		<p>third party</p> <p>(iii) The means or method of provision to a third party</p> <p>(iv) The fact that the provision of such personal data as will lead to the identification of the person to a third party will be discontinued at the request of the person</p> <p>(4) In following the cases, the individual or business operator receiving such personal data shall not be deemed a third party for the purpose of application of the provisions of the preceding three paragraphs:</p> <p>(i) Cases in which a business operator handling personal information entrust the handling of personal data in whole or in part within the scope necessary for the achievement of the Purpose of Utilization</p> <p>(ii) Cases in which personal data is provided as a result of the succession of business in a merger or otherwise</p> <p>(iii) Cases in which personal data is used jointly between specific individuals or entities and in which this fact, the items of the personal data used jointly, the scope of the joint users, the purpose for which the personal data is used by them, and the name of the individual or business operator responsible for the management of the personal data is, in advance, notified to the person or put in a readily accessible condition for the person.</p>
<p>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?</p> <p>If YES, describe.</p>		<p>ACT</p> <p>Article 16</p> <p>(1) A business operator handling personal information shall not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Utilization specified pursuant to the provision of the preceding article.</p>

<p>13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances?</p> <p>13.a) Based on express consent of the individual?</p> <p>13.b) Necessary to provide a service or product requested by the individual?</p> <p>13.c) Compelled by applicable laws?</p>	<p>Where applicant answers NO to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes.</p> <p>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:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>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.</p> <p>Where the Applicant answers YES to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is</p>	<p>ACT</p> <p>Article 16</p> <p>(1) A business operator handling personal information shall not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Utilization specified pursuant to the provision of the preceding article.</p> <p>(3) The provisions of the preceding two paragraphs shall not apply to the following cases:</p> <ul style="list-style-type: none"> (i) Cases in which the handling of personal information is based on laws and regulations (ii) Cases in which the handling of personal information is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person. (iii) Cases in which the handling of personal information is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person (iv) Cases in which the handling of personal information is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by either of the former two in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person is likely to impede the execution of the affairs concerned <p>Article 23</p> <p>(1) A business operator handling personal information shall not, except in the following cases, provide personal</p>
---	---	---

	<p>bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement.</p> <p>Where the Applicant answers NO to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.</p>	<p>data to a third party without obtaining the prior consent of the person:</p> <ul style="list-style-type: none">(i) Cases in which the provision of personal data is based on laws and regulations(ii) Cases in which the provision of personal data is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person(iii) Cases in which the provision of personal data is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person(iv) Cases in which the provision of personal data is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by one in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person are likely to impede the execution of the affairs <p>Article 18</p> <p>(1)When having acquired personal information, a business operator handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of Utilization.</p> <p>(2)Notwithstanding the provision of the preceding paragraph, when a business operator handling personal information acquires such personal information on a person as is written in a contract or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. hereinafter the same shall apply in this paragraph.) as a result of concluding a contract with the</p>
--	--	---

		<p>person or acquires such personal information on a person as is written in a document directly from the person, the business operator shall expressly show the Purpose of Utilization in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.</p> <p>(3)When a business operator handling personal information has changed the Purpose of Utilization, the business operator shall notify the person of the changed Purpose of Utilization or publicly announce it.</p> <p>(4)The provisions of the preceding three paragraphs shall not apply to the following cases:</p> <ul style="list-style-type: none">(i) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the life, body, property, or other rights or interests of the person or a third party(ii) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the rights or legitimate interests of the business operator handling personal information(iii) Cases in which it is necessary to cooperate with a state organ or a local government in executing the affairs prescribed by laws and regulations and in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to impede the execution of the affairs(iv) Cases in which it is considered that the Purpose of Utilization is clear in consideration of the circumstances of the acquisition
--	--	--

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. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	JOP Finding
<p>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?</p> <p>Where YES describe such mechanisms below.</p>	<p>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:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated.</p> <p>Where the Applicant answers NO, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable</p>	<p>ACT</p> <p>Article 16 (1): An entity handling personal information must not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the purpose of use, specified under the preceding Article.</p> <p>Article 17 A business operator handling personal information shall not acquire personal information by a deception or other wrongful means.</p> <p>BASIC POLICY</p> <p>Article 6(1)a: To maintain the society's trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy to understand manner,</p>

	<p>qualification is justified.</p> <p>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.</p>	<p>their procedures related to the handling of personal information, such as notification and announcement of the purpose of use and disclosure etc., as well as comply with the relevant laws and ordinances.</p> <p>Article 6(1)b: From the viewpoint of the protection of the rights and interests of the concerned persons, important to further improve response to the requests of concerned persons, such as consumers etc., in the policies and philosophies on the promotion of personal information protection...by including statements that consider the following points:...</p> <ul style="list-style-type: none"> • Whether information is entrusted to others or not, promoting the clarification of outside processing, such as clarifying the details of work done outside the business by outsourcers; • Specifying as concretely as possible the source the personal information was acquired from and the method of acquisition (the type of acquisition source etc.)
<p>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?</p> <p>Where YES describe such mechanisms below.</p>	<p>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:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) 	<p>ACT</p> <p>Article 16 (1): An entity handling personal information must not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the purpose of use, specified under the preceding Article.</p> <p>Article 24 (1) With respect to the retained personal data, an entity handling personal information must put the matters enumerated in the following items in an accessible condition for the person:...</p> <p>(ii) the purpose of use of all retained personal data...</p>

	<p>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.</p> <p>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.</p> <p>Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before:</p> <ul style="list-style-type: none">• 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. <p>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.</p> <p>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.</p>	<p><i>BASIC POLICY</i></p> <p>Article 6(1)a: To maintain the society’s trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy to understand manner, their procedures related to the handling of personal information, such as notification and announcement of the purpose of use and disclosure etc., as well as comply with the relevant laws and ordinances.</p> <p>Article 6(1)b: From the viewpoint of the protection of the rights and interests of the concerned persons, important to further improve response to the requests of concerned persons, such as consumers etc., in the policies and philosophies on the promotion of personal information protection...by including statements that consider the following points:...</p> <ul style="list-style-type: none">• Whether information is entrusted to others or not, promoting the clarification of outside processing, such as clarifying the details of work done outside the business by outsourcers;• Specifying as concretely as possible the source the personal information was acquired from and the method of acquisition (the type of acquisition source etc.)
--	--	--

<p>16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information?</p> <p>Where YES describe such mechanisms below.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>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.</p> <p>Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information.</p> <p>Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before:</p> <ul style="list-style-type: none"> • 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 	<p>ACT</p> <p>Article 16 (1): An entity handling personal information must not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the purpose of use, specified under the preceding Article.</p> <p>BASIC POLICY</p> <p>Article 6(1)a: To maintain the society’s trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy to understand manner, their procedures related to the handling of personal information, such as notification and announcement of the purpose of use and disclosure etc., as well as comply with the relevant laws and ordinances.</p>

	<p>and conspicuous manner, or compatible with that for which the information was collected.</p> <p>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.</p> <p>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.</p>	
<p>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?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner.</p> <p>Where the Applicant answers NO, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.</p>	<p>ACT</p> <p>Article 18 (2): Notwithstanding the provision of the preceding paragraph, when a business operator handling personal information acquires such personal information on a person as is written in a contract or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. hereinafter the same shall apply in this paragraph.) as a result of concluding a contract with the person or acquires such personal information on a person as is written in a document directly from the person, the business operator shall expressly show the Purpose of Utilization in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.</p> <p>BASIC POLICY</p>

		<p>Article 6(1)a: To maintain the society’s trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy to understand manner, their procedures related to the handling of personal information, such as notification and announcement of the purpose of use and disclosure etc., as well as comply with the relevant laws and ordinances.</p>
<p>18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant’s choice mechanism is clearly worded and easily understandable.</p> <p>Where the Applicant answers NO, and/or when the Accountability Agent finds that the Applicant’s choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.</p>	<p>ACT</p> <p>Article 18 (2): Notwithstanding the provision of the preceding paragraph, when a business operator handling personal information acquires such personal information on a person as is written in a contract or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. hereinafter the same shall apply in this paragraph.) as a result of concluding a contract with the person or acquires such personal information on a person as is written in a document directly from the person, the business operator shall expressly show the Purpose of Utilization in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.</p> <p>BASIC POLICY</p> <p>Article 6(1)a: To maintain the society’s trust of business</p>

		<p>activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy to understand manner, their procedures related to the handling of personal information, such as notification and announcement of the purpose of use and disclosure etc., as well as comply with the relevant laws and ordinances</p>
<p>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.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable.</p> <p>Where the Applicant answers NO, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.</p>	<p>ACT</p> <p>Article 18 (2): Notwithstanding the provision of the preceding paragraph, when a business operator handling personal information acquires such personal information on a person as is written in a contract or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. hereinafter the same shall apply in this paragraph.) as a result of concluding a contract with the person or acquires such personal information on a person as is written in a document directly from the person, the business operator shall expressly show the Purpose of Utilization in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.</p> <p>Article 24 (3) When an entity handling personal information has decided not to notify the Purpose of Utilization of such retained personal data as is requested under the preceding paragraph, the entity must notify the person of that effect</p>

		<p>without delay.</p> <p>Article 30 (2) When a business operator handling personal information collects charges pursuant to the provision of the preceding paragraph, the business operator shall determine the amounts of charges within the scope considered reasonable in consideration of actual costs.</p> <p><i>BASIC POLICY</i></p> <p>Article 6(1)a: To maintain the society’s trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy to understand manner, their procedures related to the handling of personal information, such as notification and announcement of the purpose of use and disclosure etc., as well as comply with the relevant laws and ordinances</p>
<p>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.</p> <p>Describe below.</p>	<p>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.</p> <p>Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p><i>ACT</i></p> <p>Article 18 (2) Notwithstanding the provision of the preceding paragraph, when a business operator handling personal information acquires such personal information on a person as is written in a contract or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. hereinafter the same shall apply in this paragraph.) as a result of concluding a contract with the person or acquires such personal information on a person</p>

	<p>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.</p>	<p>as is written in a document directly from the person, the business operator shall expressly show the Purpose of Utilization in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.</p> <p><i>BASIC POLICY</i></p> <p>Article 6(1)a: To maintain the society’s trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy to understand manner, their procedures related to the handling of personal information, such as notification and announcement of the purpose of use and disclosure etc., as well as comply with the relevant laws and ordinances.</p>
--	--	---

INTEGRITY OF PERSONAL INFORMATION

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

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
<p>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?</p> <p>If YES, describe.</p>	<p>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.</p> <p>The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use.</p> <p>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.</p>	<p>ACT</p> <p>Article 19 A business operator handling personal information shall endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Utilization</p>
<p>22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use?</p>	<p>Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information</p>	<p>ACT</p> <p>Article 19 A business operator handling personal information shall endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the</p>

<p>Provide a description in the space below or in an attachment if necessary.</p>	<p>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.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.</p>	<p>Purpose of Utilization.</p> <p>Article 26 (1) When a business operator handling personal information is requested by a person to correct, add, or delete such retained personal data as may lead to the identification of the person on the ground that the retained personal data is contrary to the fact, the business operator shall, except in cases in which special procedures are prescribed by any other laws and regulations for such correction, addition, or deletion, make a necessary investigation without delay within the scope necessary for the achievement of the Purpose of Utilization and, on the basis of the results, correct, add, or delete the retained personal data.</p>
<p>23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred?</p> <p>If YES, describe.</p>	<p>Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf.</p> <p>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.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information</p>	<p>ACT</p> <p>Article 19 A business operator handling personal information shall endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Utilization.</p> <p>Article 22 When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.</p> <p>BASIC POLICY</p> <p>6(1)c: It is important to prepare mechanisms to ensure an internal accountability system in the business for the safe management of personal information, such as the establishment of a personal information manager, the</p>

	<p>was transferred, are required for compliance with this principle.</p>	<p>management of internal access, and measures to prevent information from being taken out of the business, in addition to measures to prevent the improper access of information by outside parties. Also when handling personal information is entrusted to an outside party, it is important to ensure an effective system of oversight, including oversight in cases where information is re-entrusted to another party, by clearly establishing in the outsourcing agreement, the responsibilities of both the trustee and the entrusting entity.</p>
<p>24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed?</p> <p>If YES, describe.</p>	<p>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.</p> <p>The Accountability Agent must verify that these procedures are in place and operational.</p> <p>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.</p>	<p>ACT</p> <p>Article 19 A business operator handling personal information shall endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Utilization.</p> <p>Article 22 When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.</p>
<p>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</p>	<p>Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform</p>	<p>ACT</p> <p>Article 19 A business operator handling personal information shall endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Utilization.</p>

<p>out-of-date?</p>	<p>the Applicant about any personal information known to be inaccurate incomplete, or outdated.</p> <p>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.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.</p>	<p>Article 22</p> <p>When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.</p>
---------------------	--	---

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?	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of this written policy.</p> <p>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.</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p>
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	<p>Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include:</p> <ul style="list-style-type: none"> • Authentication and access control (eg password protections) • Encryption • Boundary protection (eg firewalls, intrusion detection) • Audit logging • Monitoring (eg external and internal audits, vulnerability scans) 	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p>

	<ul style="list-style-type: none"> • Other (specify) <p>The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant’s size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.</p> <p>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.</p> <p>The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.</p> <p>Where the Applicant indicates that it has NO physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.</p>	
<p>28. Describe how the safeguards you identified in response to question 27 are proportional to the</p>	<p>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</p>	<p>ACT</p> <p>Article 20</p> <p>A business operator handling personal information shall</p>

<p>likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.</p>	<p>safeguards are proportional to the risks identified.</p> <p>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.</p>	<p>take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p> <p>Article 21 When a business operator handling personal information has an employee handle personal data, it shall exercise necessary and appropriate supervision over the employee to ensure the security control of the personal data.</p> <p><i>BASIC POLICY</i></p> <p>6(1)c: It is important to prepare mechanisms to ensure an internal accountability system in the business for the safe management of personal information, such as the establishment of a personal information manager, the management of internal access, and measures to prevent information from being taken out of the business, in addition to measures to prevent the improper access of information by outside parties. Also when handling personal information is entrusted to an outside party, it is important to ensure an effective system of oversight, including oversight in cases where information is re-entrusted to another party, by clearly establishing in the outsourcing agreement, the responsibilities of both the trustee and the entrusting entity.</p> <p>6(1)e: In order to ensure the appropriate protection of personal information handled at a business, it is important to take necessary and appropriate measures in accordance with the risk caused by the nature of the business and the status of the handling of personal data, and to consider the size of the infringement of the rights and interests borne by the concerned persons in the event of the disclosure,</p>
---	--	--

		loss or damage etc. of personal information.
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).	<p>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:</p> <ul style="list-style-type: none"> • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) <p>Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p> <p>Article 21 When a business operator handling personal information has an employee handle personal data, it shall exercise necessary and appropriate supervision over the employee to ensure the security control of the personal data.</p> <p>BASIC POLICY</p> <p>6(1)d: In order to ensure the appropriate protection of personal information handled at businesses, such as the prevention of its disclosure, it is important to make employees fully aware of the protection of personal information by enlightening employees who handle personal information in their actual duties through the implementation of education and training etc.</p>
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:	<p>Where the Applicant answers YES (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards.</p> <p>The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information.</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p> <p>Article 21</p>

<p>30.a) Employee training and management or other safeguards?</p> <p>30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?</p> <p>30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?</p> <p>30.d) Physical security?</p>	<p>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.</p>	<p>When a business operator handling personal information has an employee handle personal data, it shall exercise necessary and appropriate supervision over the employee to ensure the security control of the personal data.</p> <p><i>BASIC POLICY</i></p> <p>6(1)c: It is important to prepare mechanisms to ensure an internal accountability system in the business for the safe management of personal information, such as the establishment of a personal information manager, the management of internal access, and measures to prevent information from being taken out of the business, in addition to measures to prevent the improper access of information by outside parties. Also when handling personal information is entrusted to an outside party, it is important to ensure an effective system of oversight, including oversight in cases where information is re-entrusted to another party, by clearly establishing in the outsourcing agreement, the responsibilities of both the trustee and the entrusting entity.</p> <p>6(1)d: In order to ensure the appropriate protection of personal information handled at businesses, such as the prevention of its disclosure, it is important to make employees fully aware of the protection of personal information by enlightening employees who handle personal information in their actual duties through the implementation of education and training etc.</p> <p>6(1)e: In order to ensure the appropriate protection of personal information handled at a business, it is important to take necessary and appropriate measures in accordance with the risk caused by the nature of the business and the status of the handling</p>
---	--	--

		<p>of personal data, and to consider the size of the infringement of the rights and interests borne by the concerned persons in the event of the disclosure, loss or damage etc. of personal information.</p>
<p>31. Have you implemented a policy for secure disposal of personal information?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p> <p>BASIC POLICY</p> <p>6(1)c: It is important to prepare mechanisms to ensure an internal accountability system in the business for the safe management of personal information, such as the establishment of a personal information manager, the management of internal access, and measures to prevent information from being taken out of the business, in addition to measures to prevent the improper access of information by outside parties. Also when handling personal information is entrusted to an outside party, it is important to ensure an effective system of oversight, including oversight in cases where information is re-entrusted to another party, by clearly establishing in the outsourcing agreement, the responsibilities of both the trustee and the entrusting entity.</p> <p>6(1)e: In order to ensure the appropriate protection of personal information handled at a business, it is important to take necessary and appropriate measures in accordance with the risk caused by the nature of the business and the status of the handling</p>

		<p>of personal data, and to consider the size of the infringement of the rights and interests borne by the concerned persons in the event of the disclosure, loss or damage etc. of personal information.</p>
<p>32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?</p>	<p>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.</p> <p>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.</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p> <p>BASIC POLICY</p> <p>6(1)c: It is important to prepare mechanisms to ensure an internal accountability system in the business for the safe management of personal information, such as the establishment of a personal information manager, the management of internal access, and measures to prevent information from being taken out of the business, in addition to measures to prevent the improper access of information by outside parties. Also when handling personal information is entrusted to an outside party, it is important to ensure an effective system of oversight, including oversight in cases where information is re-entrusted to another party, by clearly establishing in the outsourcing agreement, the responsibilities of both the trustee and the entrusting entity.</p> <p>6(1)d: In order to ensure the appropriate protection of personal information handled at businesses, such as the prevention of its disclosure, it is important to make employees fully aware of the protection of personal information by enlightening employees who handle personal information in their actual</p>

		<p>duties through the implementation of education and training etc.</p> <p>6(1)e: In order to ensure the appropriate protection of personal information handled at a business, it is important to take necessary and appropriate measures in accordance with the risk caused by the nature of the business and the status of the handling of personal data, and to consider the size of the infringement of the rights and interests borne by the concerned persons in the event of the disclosure, loss or damage etc. of personal information.</p>
<p>33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.</p>	<p>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.</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p> <p>Article 21 When a business operator handling personal information has an employee handle personal data, it shall exercise necessary and appropriate supervision over the employee to ensure the security control of the personal data.</p>
<p>34. Do you use risk assessments or third-party certifications? Describe below.</p>	<p>The Accountability Agent must verify that such risk assessments or 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</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p>

	implemented.	<p>Article 22 When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.</p>
<p>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:</p> <p>35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?</p> <p>35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information</p>	<p>The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p> <p>Article 21 When a business operator handling personal information has an employee handle personal data, it shall exercise necessary and appropriate supervision over the employee to ensure the security control of the personal data.</p> <p>Article 22 When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.</p> <p><i>Note: Article 22 of the Act obliges business operators exercise necessary supervision over the trustee. Accordingly, business operators are expected to have an arrangement in which the trustee notifies the business operators when they become aware of a breach of the</i></p>

<p>of the Applicant's customers?</p> <p>35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?</p>		<p><i>privacy or security of the information.</i></p> <p><i>BASIC POLICY</i></p> <p>6(1)e: In order to ensure the appropriate protection of personal information handled at a business, it is important to take necessary and appropriate measures in accordance with the risk caused by the nature of the business and the status of the handling of personal data, and to consider the size of the infringement of the rights and interests borne by the concerned persons in the event of the disclosure, loss or damage etc. of personal information.</p>
---	--	--

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. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
<p>36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual?</p> <p>Describe below.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests.</p> <p>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.</p> <p>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.</p> <p>The personal information must be provided to individuals in an easily comprehensible way.</p>	<p>ACT</p> <p>Article 25 (1) When a business operator handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person (such disclosure includes notifying the person that the business operator has no such retained personal data as may lead to the identification of the person concerned. The same shall apply hereinafter.), the business operator shall disclose the retained personal data without delay by a method prescribed by a Cabinet Order. However, in falling under any of the following items, the business operator may keep all or part of the retained personal data undisclosed: (i) Cases in which disclosure is likely to harm the life, body, property, or other rights or interests of</p>

	<p>The Applicant must provide the individual with a time frame indicating when the requested access will be granted.</p> <p>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.</p> <p>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>the person or a third party</p> <ul style="list-style-type: none"> (ii) Cases in which disclosure is likely to seriously impede the proper execution of the business of the business operator handling personal information (iii) Cases in which disclosure violates other laws and regulations
<p>37. Upon request, do you provide individuals access to the personal information that you hold about them?</p> <p>Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests.</p> <p>Where NO, proceed to question 38.</p> <p>37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.</p>	<p>Where the Applicant answers YES the Accountability Agent must verify each answer provided.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<p>ACT</p> <p>Article 25</p> <p>(1) When a business operator handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person (such disclosure includes notifying the person that the business operator has no such retained personal data as may lead to the identification of the person concerned. The same shall apply hereinafter.), the business operator shall disclose the retained personal data without delay by a method prescribed by a Cabinet Order. However, in falling under any of the following items, the business operator may keep all or part of the retained personal data undisclosed:</p> <ul style="list-style-type: none"> (i) Cases in which disclosure is likely to harm the life, body, property, or other rights or interests of the person or a third party (ii) Cases in which disclosure is likely to seriously impede the proper execution of the business of the business operator handling personal information

<p>37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe.</p> <p>37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.</p> <p>37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)?</p> <p>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.</p>	<p>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>(iii) Cases in which disclosure violates other laws and regulations</p> <p>Article 29 (4) When an entity determine the procedures for meeting requests for disclosure and others under the provisions of the preceding three paragraphs, the entity must take into consideration that the procedures will not impose excessively heavy burden on the persons making requests for disclosure and others.</p> <p>Article 30 (2) When a business operator handling personal information collects charges pursuant to the provision of the preceding paragraph, the business operator shall determine the amounts of charges within the scope considered reasonable in consideration of actual costs.</p> <p>CABINET ORDER</p> <p>Article 6: The method specified by a Cabinet Order under paragraph 1 of Article 25 of the Act shall be the provision of documents or the method agreed upon by the person requesting disclosure, if any.</p> <p>Note: <i>Article 6 of the Cabinet Order stipulates that business operators shall disclose retained personal data in writing unless the concerned person agrees upon other measure for the disclosure.</i></p> <p>Article 7: Matters concerning procedures for receiving requests for disclosure and others that an entity handling personal information may determine pursuant to the provision of Paragraph 1 of Article 29 of the Act shall be as set forth below:</p> <p>(1) The place where requests for disclosure and others</p>
--	--	--

		<p>are to be filed;</p> <p>(2) Format of the documents including records made by an electronic record, magnetic method or any other methods not recognizable to human senses to be submitted and other methods of making requests for disclosure and others at the time of making requests for disclosure and others;</p> <p>(3) Methods of identifying a person making requests for disclosure and others as the principal or representative prescribed in the following Article;</p> <p>(4) Methods of collecting charges set forth in paragraph 1 of Article 30 of the Act.</p>
<p>38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted?</p> <p>Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e).</p> <p>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.</p> <p>38.b) If an individual demonstrates that personal information</p>	<p>Where the Applicant answers YES to questions 38a to 38e, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy.</p> <p>If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate.</p> <p>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.</p> <p>Where the Applicant answers NO to questions 38a-</p>	<p>ACT</p> <p>Article 26</p> <p>(1) When a business operator handling personal information is requested by a person to correct, add, or delete such retained personal data as may lead to the identification of the person on the ground that the retained personal data is contrary to the fact, the business operator shall, except in cases in which special procedures are prescribed by any other laws and regulations for such correction, addition, or deletion, make a necessary investigation without delay within the scope necessary for the achievement of the Purpose of Utilization and, on the basis of the results, correct, add, or delete the retained personal data.</p> <p>Article 28</p> <p>When a business operator handling personal information notifies a person requesting the business operator to take certain measures pursuant to the provisions of paragraph (3) of Article 24, paragraph (2) of Article 25, paragraph (2) of Article 26, or paragraph (3) of the preceding article that the business operator</p>

<p>about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion?</p> <p>38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?</p> <p>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?</p> <p>38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?</p>	<p>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.</p> <p>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>will not take all or part of the measures or that the business operator will take different measures, the business operator shall endeavor to explain the reasons.</p> <p><i>CABINET ORDER</i></p> <p>Article 6: The method specified by a Cabinet Order under paragraph 1 of Article 25 of the Act shall be the provision of documents or the method agreed upon by the person requesting disclosure, if any.</p> <p><i>Note: Article 6 of the Cabinet Order stipulates that business operators shall disclose retained personal data in writing unless the concerned person agrees upon other measure for the disclosure.</i></p> <p>Article 7: Matters concerning procedures for receiving requests for disclosure and others that an entity handling personal information may determine pursuant to the provision of Paragraph 1 of Article 29 of the Act shall be as set forth below:</p> <ol style="list-style-type: none"> (1) The place where requests for disclosure and others are to be filed; (2) Format of the documents including records made by an electronic record, magnetic method or any other methods not recognizable to human senses to be submitted and other methods of making requests for disclosure and others at the time of making requests for disclosure and others; (3) Methods of identifying a person making requests for disclosure and others as the principal or representative prescribed in the following Article; (4) Methods of collecting charges set forth in paragraph 1 of Article 30 of the Act.
--	--	---

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 (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
<p>39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe.</p> <ul style="list-style-type: none"> • Internal guidelines or policies (if applicable, describe how implemented) ___ • Contracts ___ • Compliance with applicable industry or sector laws and regulations ___ 	<p>The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p> <p>BASIC POLICY</p> <p>6(1)c: It is important to prepare mechanisms to ensure an internal accountability system in the business for the safe management of personal information, such as the establishment of a personal information manager, the management of internal access, and measures to prevent information from being taken out of the business, in addition to measures to prevent the improper access of information by outside parties. Also when handling</p>

<ul style="list-style-type: none"> • Compliance with self-regulatory applicant code and/or rules ___ • Other (describe) ___ 		<p>personal information is entrusted to an outside party, it is important to ensure an effective system of oversight, including oversight in cases where information is re-entrusted to another party, by clearly establishing in the outsourcing agreement, the responsibilities of both the trustee and the entrusting entity.</p>
<p>40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?</p>	<p>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.</p> <p>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.</p> <p>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.</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p> <p>BASIC POLICY</p> <p>6(1)c: It is important to prepare mechanisms to ensure an internal accountability system in the business for the safe management of personal information, such as the establishment of a personal information manager, the management of internal access, and measures to prevent information from being taken out of the business, in addition to measures to prevent the improper access of information by outside parties. Also when handling personal information is entrusted to an outside party, it is important to ensure an effective system of oversight, including oversight in cases where information is re-entrusted to another party, by clearly establishing in the outsourcing agreement, the responsibilities of both the trustee and the entrusting entity.</p>
<p>41. Do you have procedures in place to receive, investigate and respond to privacy- related complaints?</p>	<p>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:</p>	<p>ACT</p> <p>Article 31 (1) A business operator handling personal information shall endeavor to appropriately and</p>

<p>Please describe.</p>	<ol style="list-style-type: none"> 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.</p>	<p>promptly process complaints about the handling of personal information.</p> <p>(2) A business operator handling personal information shall endeavor to establish a system necessary for achieving the purpose set forth in the preceding paragraph.</p>
<p>42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?</p>	<p>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.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.</p>	<p>ACT</p> <p>Article 31</p> <p>(1) A business operator handling personal information shall endeavor to appropriately and promptly process complaints about the handling of personal information.</p> <p>(2) A business operator handling personal information shall endeavor to establish a system necessary for achieving the purpose set forth in the preceding paragraph.</p> <p>BASIC POLICY</p>

		<p>Article 7(1): For complaint processing, the law makes it clear, that first of all, in the responsibilities of business that handle personal information, is the appropriate and swift processing of complaints. In order to fulfill these obligations, it is requested that businesses establish a point of contact for complaints and formulate complaint processing procedures as necessary system preparations.</p>
<p>43. If YES, does this response include an explanation of remedial action relating to their complaint?</p> <p>Describe.</p>	<p>The Accountability Agent must verify that the Applicant indicates what remedial action is considered.</p>	<p>ACT</p> <p>Article 31 (1) A business operator handling personal information shall endeavor to appropriately and promptly process complaints about the handling of personal information. (2) A business operator handling personal information shall endeavor to establish a system necessary for achieving the purpose set forth in the preceding paragraph.</p> <p><i>Note: Article 31(1) and (2) are interpreted as capturing a requirement that the business operator provide individuals with an explanation of the remedial action taken as a result of their complaint, as required under CBPR Program Requirement 43.</i></p>
<p>44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints?</p> <p>If YES, describe.</p>	<p>Where the Applicant answers YES, the Accountability Agent 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.</p> <p>Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures,</p>	<p>ACT</p> <p>Article 31 (1) A business operator handling personal information shall endeavor to appropriately and promptly process complaints about the handling of personal information. (2) A business operator handling personal information shall endeavor to establish a system necessary for achieving the purpose set forth in the</p>

	<p>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.</p>	<p>preceding paragraph.</p> <p>BASIC POLICY</p> <p>6(1)d: In order to ensure the appropriate protection of personal information handled at businesses, such as the prevention of its disclosure, it is important to make employees fully aware of the protection of personal information by enlightening employees who handle personal information in their actual duties through the implementation of education and training etc.</p> <p>Article 7(1): For complaint processing, the law makes it clear, that first of all, in the responsibilities of business that handle personal information, is the appropriate and swift processing of complaints. In order to fulfill these obligations, it is requested that businesses establish a point of contact for complaints and formulate complaint processing procedures as necessary system preparations.</p>
<p>45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.</p>	<p>ACT</p> <p>Article 16</p> <p>(1) A business operator handling personal information shall not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Utilization specified pursuant to the provision of the preceding article.</p> <p>(3) The provisions of the preceding two paragraphs shall not apply to the following cases:</p> <p>(i) Cases in which the handling of personal information is based on laws and regulations</p> <p>Article 23</p> <p>(1) A business operator handling personal information</p>

		<p>shall not, except in the following cases, provide personal data to a third party without obtaining the prior consent of the person:</p> <p>(i) Cases in which the provision of personal data is based on laws and regulations</p>
<p>46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?</p> <ul style="list-style-type: none"> • Internal guidelines or policies ___ • Contracts ___ • Compliance with applicable industry or sector laws and regulations ___ • Compliance with self-regulatory applicant code and/or rules ___ • Other (describe) ___ 	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of each type of agreement described.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.</p>	<p>ACT</p> <p>Article 22</p> <p>When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.</p>

<p>47. Do these agreements generally require that personal information processors, agents, contractors or other service providers:</p> <ul style="list-style-type: none"> • Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement? _____ • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? ___ • Follow instructions provided by you relating to the manner in which your personal information must be handled? ____ • Impose restrictions on subcontracting unless with your consent? ___ . • Have their CBPRs certified by an APEC accountability agent in their jurisdiction? ___ • Notify the Applicant in 	<p>The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.</p>	<p>ACT</p> <p>Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.</p> <p>Article 22 When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.</p>
--	--	--

<p>the case of a breach of the personal information of the Applicant's customers? __</p> <ul style="list-style-type: none"> • Other (describe) 		
<p>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?</p> <p>If YES, describe below.</p>	<p>The Accountability Agent must verify the existence of such self-assessments.</p>	<p>ACT</p> <p>Article 22 When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.</p>
<p>49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other services providers to ensure compliance with your instructions and/or agreements/contracts?</p> <p>If yes, describe.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms.</p> <p>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.</p>	<p>ACT</p> <p>Article 22 When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.</p>
<p>50. Do you disclose personal information to other recipient persons or organizations in situations where due diligence and reasonable steps to ensure compliance with your</p>	<p>If YES, the Accountability Agent must ask the Applicant to explain:</p> <p>(1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and</p>	<p>ACT</p> <p>Article 23 (1) A business operator handling personal information shall not, except in the following cases, provide personal data to a third party without obtaining the prior consent of the person:</p>

<p>APEC CBPRs by the recipient as described above is impractical or impossible?</p>	<p>(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.</p>	<ul style="list-style-type: none"> (i) Cases in which the provision of personal data is based on laws and regulations (ii) Cases in which the provision of personal data is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person (iii) Cases in which the provision of personal data is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person (iv) Cases in which the provision of personal data is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by one in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person are likely to impede the execution of the affairs <p>(2) With respect to personal data intended to be provided to a third party, where a business operator handling personal information agrees to discontinue, at the request of a person, the provision of such personal data as will lead to the identification of the person, and where the business operator, in advance, notifies the person of the matters listed in the following items or put those matters in a readily accessible condition for the person, the business operator may, notwithstanding the provision of the preceding paragraph, provide such personal data to a third party:</p> <ul style="list-style-type: none"> (i) The fact that the provision to a third party is the Purpose of Utilization (ii) The items of the personal data to be provided to a third party (iii) The means or method of provision to a third party (iv) The fact that the provision of such personal data as will lead to the identification of the person to a third
---	--	---

		<p>party will be discontinued at the request of the person</p> <p>(3) When a business operator handling personal information changes the matter listed in item (ii) or (iii) of the preceding paragraph, the business operator shall, in advance, notify the person of the content of the change or put it in a readily accessible condition for the person.</p> <p>(4) In following the cases, the individual or business operator receiving such personal data shall not be deemed a third party for the purpose of application of the provisions of the preceding three paragraphs:</p> <ul style="list-style-type: none"> (i) Cases in which a business operator handling personal information entrust the handling of personal data in whole or in part within the scope necessary for the achievement of the Purpose of Utilization (ii) Cases in which personal data is provided as a result of the succession of business in a merger or otherwise (iii) Cases in which personal data is used jointly between specific individuals or entities and in which this fact, the items of the personal data used jointly, the scope of the joint users, the purpose for which the personal data is used by them, and the name of the individual or business operator responsible for the management of the personal data is, in advance, notified to the person or put in a readily accessible condition for the person.
--	--	---

Further Explanations - Selected Provisions:

- *Article 2(6) of the Act provides definition of “person”. A “person” can be considered as the same thing as the “data subject”.*
- *According to Article 18(1) of the Act, business operators are required to publicly announce or promptly notify the purpose of utilization of personal data which they acquire either directly or indirectly from consumers. In addition, Article 18(2) obliges business operators, when*

they acquire personal data directly from a person in writing, to expressly explain the purpose of utilization of his/her personal data. Article 18(2) provides an extra measure to ensure the notification of the purpose of utilization of personal data to be made obvious to consumers. As well Article 18(2) of the Act provides several options for exercising choice (written contract, record made by electric or magnetic method, etc.)

- *Article 23(2) of the Act stipulates Opt Out conditions under the Act. When business operators notify consumers in advance of matters (i) to (iv) or when they put those matters in a readily accessible condition for consumers, business operators are allowed to provide personal data to third parties.*
- *Article 23(4) of the Act stipulates exceptions in which business operators are allowed to provide personal data to other entities. These are limited to entrusted data processor (Case 1), successor of business (Case 2) or joint business partner (Case 3). In all cases, the concerned business operator is held responsible for the security of the personal data.*
- *While Article 6(1)a of the Basic Policy requests business operators to provide privacy statements to consumers, Article 6(1)b stipulates details of contents need to be covered by the privacy statements.*
- *Article 6 of the Cabinet Order stipulates that business operators shall disclose retained personal data in writing unless the concerned person agrees upon other measure for the disclosure.*
- *Article 7 of the Cabinet Order stipulates that business operators shall announce their procedures for accepting requests for disclosure, correction, etc. of retained personal data, which shall include items (1) to (4) of the Article. Consumers are expected to follow the procedures when they make such requests to business operators.*