CROSS-BORDER PRIVACY RULES SYSTEM
PARTICIPATION OF MEXICO

CROSS BORDER PRIVACY RULES SYSTEM JOINT OVERSIGHT PANEL

FINDINGS REPORT

Submitted To: Ms. Lourdes Yaptinchay
Chair, APEC Electronic Commerce Steering Group
16 January 2013

TABLE OF CONTENTS

OVERVIEW AND PURPOSE

The purpose of this findings report is to assess Mexico'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 Mexico 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 24 September 2012, Mexico's Vice Minister for Industry and Commerce for the Ministry of the Economy (herein "Economía") provided the Chair of the APEC ECSG Mexico's *Notice of Intent to Participate in the CBPR System*. The letter contained confirmation of the following:

1) The Federal Institute for Access to Information and Data Protection (herein "IFAI"), a Privacy Enforcement Authority in Mexico, is a participant in the CPEA; and

2) Mexico 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 Mexico and the enforcement authority associated with these laws and regulations; and

2) The completed APEC CBPR System Program Requirements Enforcement Map.

FINDING S OF THE JOINT OVERSIGHT PANEL

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

Having consulted with representatives from the Ministry of the Economy and the Federal Institute for Access to Information and Data Protection on the narrative description of domestic laws and regulations applicable to the certification-related activities of Accountability Agents operating in Mexico, 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 IFAI is a participant 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 Mexico.

The Cross Border Privacy Rules Joint Oversight Panel invites the Chair of the APEC ECSG to notify Mexico 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, Mexico 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.

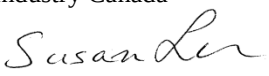
Signed,

_____

Josh Harris
Chair, Joint Oversight Panel
United States Department of Commerce

_____

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



_____

Susan Lu
Co-Chair, Joint Oversight Panel
Bureau of Foreign Trade, Chinese Taipei

16 January 2013

DISCUSSION OF FINDINGS

Letter of Intent

On 24 September 2012, the Chair of the APEC ECSG received a letter from Economía, indicating Mexico's intent to participate in the APEC Cross Border Privacy Rules (herein "CBPR") System. The letter makes the following statements:

1) IFAI is a participant in the CPEA.

2) Mexico 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 Mexican laws and regulations that may apply to any CBPR certification-related activities of an Accountability Agent operating within Mexico's jurisdiction and the enforcement authority associated with these laws and regulations.

2) The APEC CBPR System Program Requirements Enforcement Map, completed by Mexico, outlining IFAI's 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 24 September 2012 *Notice of Intent to Participate* in the APEC CBPR System, Mexico confirmed that IFAI, a Privacy Enforcement Authority in Mexico, is a participant in the CPEA.

The JOP obtained confirmation of the participation of IFAI in the CPEA from CPEA Administrators. 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 Economía, IFAI and confirmation by the CPEA Administrators, the JOP finds that Mexico 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)

Mexico's *Notice of Intent to Participate* includes a confirmation that Mexico 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 Economía 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 Mexico

Annex A of Mexico'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 Mexico. Annex A also details the enforcement authority associated with these laws, regulations and administrative measures.

Article 44 of Mexico's *Federal Law on Protection of Personal Data held by Private Parties* provides that persons or entities may agree on binding self-regulatory schemes in addition to the requirements of the Law itself. Chapter VI provides that these binding self-regulatory schemes may include third-party certification of those responsible for the protection of personal data in accordance with certification parameters established by Economía, with the support of IFAI. Article 43 grants Economía and IFAI the authority to establish and enforce these parameters, including rules governing the Certification System and the certification-related activities of third-party certifiers. Further, IFAI is granted the authority to authorize the accrediting entities that will be in charge of accrediting such certifiers.

Through the appropriate authority, Mexico 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 Mexico's *Notice of Intent to Participate* contains the completed APEC Cross- Border Privacy Rules System Program Requirements Enforcement Map. In this Map, Mexico provided citations to all relevant provisions in the *Federal Law on Protection of Personal Data held by Private Parties* and its secondary regulation, *Regulations to the Federal Law on Protection of Personal Data held by Private Parties*, that have the effect of protecting personal information consistent with the CBPR System program requirements. The Joint Oversight Panel reviewed this submission to verify the applicability of each cited Article of the Law and/or Regulation 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 Mexico's *Notice of Intent to Participate* in the CBPR System, including information provided in Annex A and Annex B, and to obtain confirmation of IFAI's participation in the CPEA. Consultations were undertaken with representatives of Economía, IFAI and Administrators of the CPEA. These consultations took place via email and teleconference.

SUSPENSION OR WITHDRAWAL OF PARTICIPATION

Participation by Mexico 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, 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.

Mexico 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 Mexico ceases participation (whether by way of withdrawal or suspension) in the CBPR System, any certifications performed by APEC-recognized Accountability Agents operating in Mexico 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 those Articles in the Federal Law on Protection of Personal Data held by Private Parties (herein 'Law') and its secondary regulation, Regulations to the Federal Law on Protection of Personal Data held by Private Parties (herein 'Regulation'), relevant to the enforceability of each of the 50 CBPR program requirements. This summary only provides the relevant text of clauses within those identified Articles necessary for the enforcement of each of the CBPR program requirements and is not intended to represent all obligations and rights provided under Mexican law.

NOTICE

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**JOP Finding**
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline. • States an effective date of Privacy Statement publication. Where Applicant answers **NO** to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent	*LAW* Article 15: The data controller will have the obligation of providing data owners with information regarding what information is collected on them and why, through the privacy notice. Article 16: The privacy notice must contain at least the following information: i. The identity and domicile of the data controller collecting the data; ii. The purposes of the data processing; iii. The options and means offered by the data controller to the data owners to limit the use or disclosure of data; iv. The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law; v. Where appropriate, the data transfers to be made, and vi. The procedure and means by which the data controller will notify the data owners of changes to the privacy notice, in accordance with the provisions of this Law. For sensitive personal data, the privacy notice must expressly state that it is dealing with this type of data. *REGULATION* Article 24: The privacy notice shall be simple, with the necessary information, written in clear and understandable language and with a structure and design that make it easy

	must verify whether the applicable qualification is justified.	to understand. Article 27: Pursuant to Article 17, section II of the Law, when personal data are collected directly from the data owner, the data controller shall immediately provide him at least with the following information: i. The identity and address of the data controller; ii. The purposes of the processing; and iii. The mechanisms offered by the data controller for the data owner to know the privacy notice in accordance with Article 26 of the Regulations hereof. The immediate distribution of the aforementioned information does not exempt the data controller from the obligation of providing mechanisms so that the data owner can know the content of the privacy notice, in compliance with Article 27 of the Regulations hereof.
1.a) Does this privacy statement describe how personal information is collected?	If **YES**, the Accountability Agent must verify that: • The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. • the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information	*LAW* Article 15: The data controller will have the obligation of providing data owners with information regarding what information is collected on them and why, through the privacy notice.

	collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*LAW* Article 15: The data controller will have the obligation of providing data owners with information regarding what information is collected on them and why, through the privacy notice.
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must notify the	*LAW* Article 16 (vi): The privacy notice must contain at least the following information…Where appropriate, the data transfers to be made… *REGULATION*: Article 68: Any transfer of personal data whether it is national or international, is subject to the consent of its data owner except in the cases provided in Article 37 of the Law and shall be communicated to him through the privacy notice and limited only to the purpose justifying it.

	Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	Article 44 (iii): The principle of loyalty establishes the obligation to process personal data favoring the protection of the data owner's interests and the reasonable expectation of privacy pursuant to Article 7 of the Law. Misleading or fraudulent means may not be used to collect and process personal data. There is fraudulent or misleading action when…(iii) The purposes were not the ones established in the privacy notice.
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a functional e-mail address. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*LAW* Article 16(i),(v): The privacy notice must contain at least the following information…(i) The identity and domicile of the data controller collecting the data;… (v) The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law… *REGULATION* Article 27 (i), (iii): Pursuant to Article 17, section II of the Law, when personal data are collected directly from the data owner, the data controller shall immediately provide him at least with the following information:…(i) The identity and address of the data controller;…(iii).The mechanisms offered by the data controller for the data owner to know the privacy notice in accordance with Article 26 of the Regulations hereof.
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant	Article 16 (i), (ii): The privacy notice must contain at least the following information: (i) The purposes of the data processing; (ii) Where appropriate, the data transfers to be made… Article 27(i): Pursuant to Article 17, section II of the Law, when personal data are collected directly from the data owner, the data controller shall immediately provide him at

	answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	least with the following information: (i) The purposes of the processing... Article 68: Any transfer of personal data whether it is national or international, is subject to the consent of its data owner except in the cases provided in Article 37 of the Law and shall be communicated to him through the privacy notice and limited only to the purpose justifying it. Article 44 (iii): The principle of loyalty establishes the obligation to process personal data favoring the protection of the data owner's interests and the reasonable expectation of privacy pursuant to Article 7 of the Law. Misleading or fraudulent means may not be used to collect and process personal data. There is fraudulent or misleading action when:…(iii) The purposes were not the ones established in the privacy notice.
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Privacy Statement includes: • The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). • The process that an individual must follow in order to correct his or her personal information 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	*LAW* Article 16 (iv): The privacy notice must contain at least the following information:…(iv) The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law.

	Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*LAW* Article 15: The data controller will have the obligation of providing data owners with information regarding what information is collected on them and why, through the privacy notice. Article 17 (I),(II): The privacy notice must be made available to data owners through print, digital, visual or audio formats or any other technology, as follows:…I. Where personal data has been obtained personally from the data owner, the privacy notice must be provided at the time the data is collected, clearly and unequivocally, through the format by which collection is carried out, unless the notice has been provided prior… II. Where personal data are obtained directly from the data owner by any electronic, optical, audio or visual means, or through any other technology, the data controller must immediately provide the data owner with at least the information referred to in sections I and II of the preceding article, as well as provide the mechanisms for the data owner to obtain the full text of the privacy notice.
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	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	*LAW* Article 15: The data controller will have the obligation of providing data owners with information regarding what information is collected on them and why, through the privacy notice.

you indicate the purpose(s) for which personal information is being collected?	communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	Article 16. The privacy notice must contain at least the following information: …II. The purposes of the data processing… Article 17 (I): The privacy notice must be made available to data owners through print, digital, visual or audio formats or any other technology, as follows:…I. Where personal data has been obtained personally from the data owner, the privacy notice must be provided at the time the data is collected, clearly and unequivocally, through the format by which collection is carried out, unless the notice has been provided prior…
4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent	*LAW* Article 16 (vi): The privacy notice must contain at least the following information:…(vi) Where appropriate, the data transfers to be made… Article 17 (I), (II): The privacy notice must be made available to data owners through print, digital, visual or audio formats or any other technology, as follows:…I. Where personal data has been obtained personally from the data owner, the privacy notice must be provided at the time the data is collected, clearly and unequivocally, through the format by which collection is carried out, unless the notice has been provided prior…II. Where personal data are obtained directly from the data owner by any electronic, optical, audio or visual means, or through any other technology, the data controller must immediately provide

	must determine whether the applicable qualification is justified.	the data owner with at least the information referred to in sections I and II of the preceding article, as well as provide the mechanisms for the data owner to obtain the full text of the privacy notice. *REGULATION* Article 68: Any transfer of personal data whether it is national or international, is subject to the consent of its data owner except in the cases provided in Article 37 of the Law and shall be communicated to him through the privacy notice and limited only to the purpose justifying it.

COLLECTION LIMITATION

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**JOP Finding**
5. How do you obtain personal information: a) Directly from the individual? b) From third parties collecting on your behalf? c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES** to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	*LAW* Article 6: Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law. Article 7: Personal data must be collected and processed in a lawful manner in accordance with the provisions established by this Law and other applicable regulations. *REGULATION* Article 10: The principle of legitimacy bounds the data controller to process the data in compliance with the Mexican legislation and international law.
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: • Each type of data collected • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data • An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection Using the above, the Accountability Agent	*LAW* Article 15: The data controller will have the obligation of providing data owners with information regarding what information is collected on them and why, through the privacy notice. Article 12: Processing of personal data must be limited to fulfillment of the purposes set out in the privacy notice. If the data controller intends to process data for another purpose which is not compatible or analogous to the purposes set out in the privacy notice, the data owner's consent must be obtained again. *REGULATION* Article 14: When the data controller intends to collect personal data directly from the data owner, he shall previously make the privacy notice available to him, which

	will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	has to include a mechanism to, be it the case, so the data owner may express his refusal to the processing of his personal data for purposes different from those necessary and drawn from a legal relationship between the data controller and the data owner….When the data controller uses mechanisms in remote or local means of electronic or optical communication or communication of another type of technology that enable him to collect personal data automatically or simultaneously as the data owner contacts them, the former shall inform the latter that personal data are collected using these technologies and how might they be disabled. Article 46: The data controller must make reasonable efforts to limit the personal data processed to the minimum necessary in accordance with the purpose of the processing taking place.
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	*LAW* Article 6: Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law. Article 7: Personal data must be collected and processed in a lawful manner in accordance with the provisions established by this Law and other applicable regulations. *REGULATION* Article 10: The principle of legitimacy bounds the data controller to process the data in compliance with the Mexican legislation and international law.

USES OF PERSONAL INFORMATION

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**JOP Finding**
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Where the Applicant 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. Where the Applicant Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	*LAW* Article 12: Processing of personal data must be limited to fulfillment of the purposes set out in the privacy notice. If the data controller intends to process data for another purpose which is not compatible or analogous to the purposes set out in the privacy notice, the data owner's consent must be obtained again. *REGULATION* Article 40: Personal data may only be processed for the compliance with the purpose or purposes set forth in the privacy notice pursuant to Article 12 of the Law. For the purposes of the foregoing paragraph, the purpose or purposes set forth in the privacy notice shall be specific, clear and objective, specifying the purpose of the processing of the personal data. Article 44 (III): The principle of loyalty establishes the obligation to process personal data favoring the protection of the data owner's interests and the reasonable expectation of privacy pursuant to Article 7 of the Law. Misleading or fraudulent means may not be used to collect and process personal data. There is fraudulent or misleading action when…(III) The purposes were not the ones established in the privacy notice. Article 46: The data controller must make reasonable efforts to limit the personal data processed to the minimum necessary in accordance with the purpose of the processing taking place.

9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. a) Based on express consent of the individual? b) Compelled by applicable laws?	Where the Applicant answers **NO** to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by	*LAW* Article 12: Processing of personal data must be limited to fulfillment of the purposes set out in the privacy notice. If the data controller intends to process data for another purpose which is not compatible or analogous to the purposes set out in the privacy notice, the data owner's consent must be obtained again. *REGULATION* Article 43 (I), (II): The data controller may not process personal data for purposes different from the ones compatible or analogous to those for which they were collected in the first place and that were set forth in the privacy notice, unless: (I) A law or regulations explicitly allows it, or (II) The data controller obtained consent for the new processing.

	law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	
10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.	Where the Applicant answers **YES** in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law. Also, the Accountability Agent must require the Applicant to identify: 1) each type of data disclosed or transferred; 2) 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.).	*LAW* Article 36: Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data. Article 37: Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases: i. Where the transfer is pursuant to a Law or Treaty to which Mexico is party; ii. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management; iii. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any

	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.	company of the same group as the data controller, operating under the same internal processes and policies; iv. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party; v. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice; vi. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and vii. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner. *REGULATION* Article 43: The data controller may not process personal data for purposes different from the ones compatible or analogous to those for which they were collected in the first place and that were set forth in the privacy notice, unless: i. A law or regulations explicitly allows it, or ii. The data controller obtained consent for the new processing.
11. Do you transfer personal information to personal information processors? If YES, describe.	*See above*	*LAW* Article 2: In addition to the definitions established in Article 3 of the Federal Law on the Protection of Personal Data Held by Private Parties, for the purposes of these Regulations, the following definitions shall apply:… IX. Transmission: Communicating personal data between a data controller and a data processor, within or outside of Mexico; …

		Article 12: Processing of personal data must be limited to fulfillment of the purposes set out in the privacy notice. If the data controller intends to process data for another purpose which is not compatible or analogous to the purposes set out in the privacy notice, the data owner's consent must be obtained again. Article 36: Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data. Article 37: Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases: i. Where the transfer is pursuant to a Law or Treaty to which Mexico is party; ii. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management; iii. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies; iv. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest

		of the data owner between the data controller and a third party; v. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice; vi. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and vii. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner. *REGULATION* Article 43: The data controller may not process personal data for purposes different from the ones compatible or analogous to those for which they were collected in the first place and that were set forth in the privacy notice, unless: i. A law or regulations explicitly allows it, or ii. The data controller obtained consent for the new processing. Article 49: The data processor is the individual or corporate body, public or private, not a part of the organization of the data controller, that alone or together with others, processes personal data on behalf of a data controller as a result of a legal relationship linking the same and setting out the scope of service to be provided. Article 53 (I). National and international transmissions of personal data between a data controller and a data processor need not be informed to the data subject or his consent obtained. The data processor shall be considered as a data controller, together with its own obligations, when

		it: I. Uses the personal data for a purpose different from that authorized by the data controller, or II. Makes a transfer without complying with the instructions of the data controller. The data processor will not be held responsible when, at the express indication of the data controller, it transmits the personal data to another data processor designated by the latter, to which it had entrusted the performance of a service, or transfers the personal data to another data controller pursuant to these Regulations.
12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.	*See above*	*LAW* Article 36: Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data. Article 37: Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases: i. Where the transfer is pursuant to a Law or Treaty to which Mexico is party; ii. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management; iii. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and

		policies; iv. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party; v. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice; vi. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and vii. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner. *REGULATION* Article 43: The data controller may not process personal data for purposes different from the ones compatible or analogous to those for which they were collected in the first place and that were set forth in the privacy notice, unless: i. A law or regulations explicitly allows it, or ii. The data controller obtained consent for the new processing.
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the	Where applicant answers **NO** to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers **YES** to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or	*LAW* Article 36: Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has

individual? 13.c) Compelled by applicable laws?	transferred for an unrelated use, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers **YES** to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers **YES** to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant answers **NO** to 13.a, b	transferred the data. Article 37: Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases: i. Where the transfer is pursuant to a Law or Treaty to which Mexico is party; ii. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management; iii. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies; iv. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party; v. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice; vi. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and vii. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner. *REGULATION* Article 43: The data controller may not process personal data for purposes different from the ones compatible or

	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.	analogous to those for which they were collected in the first place and that were set forth in the privacy notice, unless: i. A law or regulations explicitly allows it, or ii. The data controller obtained consent for the new processing.

CHOICE

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**JOP Finding**
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice	*LAW* Article 8: All processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law. Article 10: Consent for processing of personal data will not be necessary where: I. Any Law so provides; II. The data is contained in publicly available sources; III. The personal data is subject to a prior dissociation procedure; IV. It has the purpose of fulfilling obligations under a legal relationship between the data owner and the data controller; V. There is an emergency situation that could potentially harm an individual in his person or property; VI. It is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data owner is unable to give consent in the terms established by the General Health Law and other applicable laws, and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or VII. A resolution is issued by a competitive authority. Article 16 (iii),(iv): The privacy notice must contain at least the following information…(iii). The options and means offered by the data controller to the data owners to limit the use or disclosure of data…(iv). The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law…

	in relation to the collection of their personal information must be provided.	*REGULATION* Article 14: When the data controller intends to collect personal data directly from the data owner, he shall previously make the privacy notice available to him, which has to include a mechanism to, be it the case, the data owner may express his refusal to the processing of his personal data for purposes different from those necessary and drawn from a legal relationship between the data controller and the data owner….When the data controller uses mechanisms in remote or local means of electronic or optical communication or communication of another type of technology that enable him to collect personal data automatically or simultaneously as the data owner contacts them, the former shall inform the latter that personal data are collected using these technologies and how might they be disabled.
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for	*LAW* Article 16(iii), (iv): The privacy notice must contain at least the following information…(iii) The options and means offered by the data controller to the data owners to limit the use or disclosure of data…(iv). The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law; *REGULATION* Article 21: The data owner may at any time revoke his consent for the processing of his personal data, and the data controller shall establish easy and free mechanisms to allow the data owner to revoke his consent using at least the same means he used to give it, provided this is not prevented by a legal provision.

	which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before:] • being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	
16. Subject to the qualifications described below, do you provide a mechanism for individuals to	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of how	*LAW* Article 16(iii), (iv): The privacy notice must contain at least the following information…(iii) The options and

exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	individuals may exercise choice in relation to the disclosure of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection [but before disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected.] Where the Applicant answers **NO**, the Applicant must identify the applicable	means offered by the data controller to the data owners to limit the use or disclosure of data…(iv). The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law… Article 36: Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; … *REGULATION* Article 43: The data controller may not process personal data for purposes different from the ones compatible or analogous to those for which they were collected in the first place and that were set forth in the privacy notice, unless: I. A law or regulations explicitly allows it, or II. The data controller obtained consent for the new processing. Article 44 (III): The principle of loyalty establishes the obligation to process personal data favoring the protection of the data owner's interests and the reasonable expectation of privacy pursuant to Article 7 of the Law. Misleading or fraudulent means may not be used to collect and process personal data. There is fraudulent or misleading action when…(III) The purposes were not the ones established in the privacy notice.

	qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that 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.	*LAW* Article 16(iii), (iv): The privacy notice must contain at least the following information…(iii) The options and means offered by the data controller to the data owners to limit the use or disclosure of data…(iv). The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law… Article 17 (I): The privacy notice must be made available to data owners through print, digital, visual or audio formats or any other technology, as follows: (I). Where personal data has been obtained personally from the data owner, the privacy notice must be provided at the time the data is collected, clearly and unequivocally, through the format by which collection is carried out, unless the notice has been provided prior… *REGULATION* Article 24: The privacy notice shall be simple, with the necessary information, written in clear and understandable language and with a structure and design that make it easy to understand.

18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers **NO**, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	*LAW* Article 16(iii), (iv): The privacy notice must contain at least the following information…(iii) The options and means offered by the data controller to the data owners to limit the use or disclosure of data…(iv). The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law… *REGULATION* Article 24: The privacy notice shall be simple, with the necessary information, written in clear and understandable language and with a structure and design that make it easy to understand. Article 93: The exercise of ARCO rights shall be simple …. The data controller may not establish, as the only way to present requests to exercise ARCO rights, any service or means with a cost.
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	*LAW* Article 21: The data owner may at any time revoke his consent for the processing of his personal data, and the data controller shall establish easy and free mechanisms to allow the data owner to revoke his consent using at least the same means he used to give it, provided this is not prevented by a legal provision. *REGULATION* Article 14: When the data controller seeks to collect personal data directly or personally from the data subject, it shall previously make available to the data subject a privacy notice which shall contain a mechanism by which, as the case may be, the data subject may state his refusal

		to allow the processing of his personal data for purposes different from those that are necessary and that create a legal relationship between the data controller and the data subject.
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	*LAW* Article 28: The data owner or his legal representative may at any time make a request to the data controller for access, rectification, cancellation or objection in relation to the personal data concerning him. Article 30: All data controllers must designate a personal data person or department who will process requests from data owners for the exercise of the rights referred to in this Law. In addition, data controllers will promote protection of personal data within their organizations. Article 31: In the case of requests for rectification of personal data, the data owner must indicate, in addition to that which is specified in the preceding article of this Law, the changes to be made, and provide documentation supporting the request. Article 32: The data controller will notify the data owner, within a maximum of twenty days counted from the date of receipt of the request for access, rectification, cancellation or objection, of the determination made, so that, where appropriate, same will become effective within fifteen days from the date on which the notice is provided. For personal data access requests, delivery will be made upon proof of identity of the requesting party or legal representative.

INTEGRITY OF PERSONAL INFORMATION

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**JOP Finding**
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	*LAW* Article 11: The data controller shall ensure that personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected. *REGULATION* Article 36: The principle of quality is complied with when the personal data processed are exact, complete, appropriate, correct and updated as required for the compliance with the purpose of their processing. The quality of the personal data is presumed to be complied with when provided directly from the data owner and until he does not express or accredits the contrary, or when the data controller has objective evidence that contradicts the personal data. When personal data were not obtained directly from the data owner, the data controller shall take reasonable measures so the data respond to the principle of quality according to the type of personal data and the processing conditions. The data controller shall adopt the necessary mechanisms to endeavor to have exact, complete, appropriate, correct and updated personal data, in order to maintain the veracity of the information and prevent the data owner from being affected by said situation.
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for	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	*LAW* Article 16 (iv): The privacy notice must contain at least the following information…(iv) the means for exercising rights of access, rectification, cancellation

purposes of use? Provide a description in the space below or in an attachment if necessary.	and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that 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.	or objection, in accordance with the provisions of this Law. Article 30: All data designate a personal data person or department who will process requests from data owners for the exercise of the rights referred to in this Law. In addition, data controllers will promote protection of personal data within their organizations. *REGULATION* Article 36 (III), (IV):…(III) When the personal data were not obtained directly from the data subject, the data controller must take reasonable measures for it to meet the principle of quality in accordance with the type of personal data and the processing conditions. (IV) The data controller must adopt the mechanisms that it considers necessary to ensure that personal data dealt with are exact, complete, pertinent, correct, and up-to-date so that the truth of the data are not altered and the data subject thereby prejudiced by this. Article 104: …The data controller may offer mechanisms for the benefit of the data subject to facilitate the exercise of this right.
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	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.	*LAW* Article 14: The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller… Article 25:…Where personal data has been transmitted prior to the date of rectification or cancellation and continues to be processed by third parties, the data

was transferred? If YES, describe.	The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	controller must notify them of the request for rectification or cancellation, so that such third parties also carry it out. *REGULATION* Article 36: The principle of quality is complied with when the personal data processed are exact, complete, appropriate, correct and updated as required for the compliance with the purpose of their processing. The quality of the personal data is presumed to be complied with when provided directly from the data owner and until he does not express or accredits the contrary, or when the data controller has objective evidence that contradicts the personal data. When personal data were not obtained directly from the data owner, the data controller shall take reasonable measures so the data respond to the principle of quality according to the type of personal data and the processing conditions. The data controller shall adopt the necessary mechanisms to endeavor to have exact, complete, appropriate, correct and updated personal data, in order to maintain the veracity of the information and prevent the data owner from being affected by said situation. Article 72: The recipient of personal data shall abide by the Law and the Regulations hereof acting as data controller, and shall process personal data in accordance with the privacy notice informed by the transferor data controller. Article 73: The transfers shall be formalized through a mechanism showing that the transferor data controller informed the recipient data controller of the conditions

		in which the data owner consented to the processing of his personal data. Article 74: Without detriment to Article 37 of the Law, international transfers of personal data may be possible when the recipient of the personal data takes on the same obligations as the data controller who transferred the personal data. Article 75: For this purpose, the data controller who transfers the personal data may use agreements or other legal instruments providing for the same obligations as the data controller who transferred the personal data, as well as the conditions in which the data owner consented to the processing of his personal data.
24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	*LAW* Article 36: … moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data. *REGULATION* Article 36: The principle of quality is complied with when the personal data processed are exact, complete, appropriate, correct and updated as required for the compliance with the purpose of their processing. The quality of the personal data is presumed to be complied with when provided directly from the data owner and until he does not express or accredits the contrary, or when the data controller has objective evidence that contradicts the personal data. When personal data were not obtained directly from the data owner, the data controller shall take reasonable measures so the data respond to the principle of quality according to

		the type of personal data and the processing conditions. The data controller shall adopt the necessary mechanisms to endeavor to have exact, complete, appropriate, correct and updated personal data, in order to maintain the veracity of the information and prevent the data owner from being affected by said situation. Article 72: The recipient of personal data shall abide by the Law and the Regulations hereof acting as data controller, and shall process personal data in accordance with the privacy notice informed by the transferor data controller. Article 73: The transfers shall be formalized through a mechanism showing that the transferor data controller informed the recipient data controller of the conditions in which the data owner consented to the processing of his personal data. Article 74: Without detriment to Article 37 of the Law, international transfers of personal data may be possible when the recipient of the personal data takes on the same obligations as the data controller who transferred the personal data. Article 75: For this purpose, the data controller who transfers the personal data may use agreements or other legal instruments providing for the same obligations as the data controller who transferred the personal data, as well as the conditions in which the data owner consented to the processing of his personal data.
25. Do you require personal	Where the Applicant answers **YES**, the	*LAW*

information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	Article 11**:** The data controller shall ensure that personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected. Article 14: The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. *REGULATION* Article 36: The principle of quality is complied with when the personal data processed are exact, complete, appropriate, correct and updated as required for the compliance with the purpose of their processing. The quality of the personal data is presumed to be complied with when provided directly from the data owner and until he does not express or accredits the contrary, or when the data controller has objective evidence that contradicts the personal data. When personal data were not obtained directly from the data owner, the data controller shall take reasonable measures so the data respond to the principle of quality according to the type of personal data and the processing conditions. The data controller shall adopt the necessary mechanisms to endeavor to have exact, complete, appropriate, correct and updated personal data, in order to maintain the veracity of the information and prevent the data owner from being affected by said situation. Article 72: The recipient of personal data shall abide

		by the Law and the Regulations hereof acting as data controller, and shall process personal data in accordance with the privacy notice informed by the transferor data controller. Article 73: The transfers shall be formalized through a mechanism showing that the transferor data controller informed the recipient data controller of the conditions in which the data owner consented to the processing of his personal data. Article 74: Without detriment to Article 37 of the Law, international transfers of personal data may be possible when the recipient of the personal data takes on the same obligations as the data controller who transferred the personal data. Article 75: For this purpose, the data controller who transfers the personal data may use agreements or other legal instruments providing for the same obligations as the data controller who transferred the personal data, as well as the conditions in which the data owner consented to the processing of his personal data.

SECURITY SAFEGUARDS

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**JOP Finding**
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	*LAW* Article 19: All responsible parties that process personal data must establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing. Data controllers will not adopt security measures inferior to those they keep to manage their own information. Moreover, risk involved, potential consequences for the data owners, sensitivity of the data, and technological development will be taken into account. *REGULATION* Article 57: The data controller, and as applicable, the data processor, must establish and maintain administrative, physical, and if applicable technical, security measures for the protection of personal data pursuant to the Law and this Chapter, regardless of the processing system. For the purposes of this Chapter, security measures mean security control or group of controls to protect personal data. The above is without prejudice to the laws and regulations in force with respect to security issued by the competent authorities in the corresponding sector when they contemplate greater protection for data subjects than that provided in the Law and these Regulations.
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or	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	*REGULATION* Article 61: In order to guarantee the security of personal data, the data controller shall consider the following actions:

unauthorized access, destruction, use, modification or disclosure of information or other misuses?	may include: • Authentication and access control (e.g. password protections) • Encryption • Boundary protection (e.g. firewalls, intrusion detection) • Audit logging • Monitoring (e.g. external and internal audits, vulnerability scans) • Other (specify) The Applicant 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. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or	I. Prepare an inventory of personal data and of processing systems; II. Determine the functions and obligations of the persons who process personal data; III. Have a risk analysis of personal data that entails identifying dangers and estimating the risks to personal data; IV. Establish the security measures applicable to personal data and identify those implemented effectively; V. Analyze the gap/divide that consists of the difference between the existing security measures and those missing, necessary for the protection of personal data; VI. Prepare a work plan for the implementation of the missing security measures arising from the analysis of the gap/divide; VII. Carry out reviews and/or audits; VIII. Train the personnel who will carry out the processing, and IX. Keep a register of storage means of personal data.

	disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	
28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	*REGULATION* Article 60: The data controller will determine the security measures applicable to the personal data processed by him, taking the following factors into consideration: I. The inherent risk by type of personal data; II. The sensitivity of the personal data processed; III. The technological development, and IV. The possible consequences of a violation for the data owners. Moreover, the data controller shall endeavor to take the following elements into account: I. The number of data owners; II. The previous violations to the processing systems; III. The risk due to the potential quantitative or qualitative value the processed personal data may have for an unauthorized third party, and IV. Other factors that may impact the risk level or that arise from other laws or regulations applicable to

		the data controller.
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	*LAW* Article 19: All responsible parties that process personal data must establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing. Data controllers will not adopt security measures inferior to those they keep to manage their own information. Moreover, risk involved, potential consequences for the data owners, sensitivity of the data, and technological development will be taken into account. Article 30: … In addition, data controllers will promote protection of personal data within their organizations. *REGULATION* Article 48. Pursuant to Article 14 of the Law, the data controller shall adopt measures to guarantee the due processing, favoring the data owner's interests and the reasonable expectation of privacy. The measures that may be adopted by the data controller include, indicatively but without limitation thereto, the following: I. Prepare mandatory and enforceable privacy policies and programs within the data controller's organization; II. Implement a training, updating and awareness program for the personnel as regards the obligations in matters of protection of personal data; III. Establish an internal supervision and oversight system, external audits to prove the compliance with privacy policies; IV. Allocate resources to implement privacy programs

		and policies; V. Implement a procedure to address the risk for the protection of personal data due to the implementation of new products, services, technologies and business models, as well as mitigate them; VI. Periodically review the security policies and programs to determine the modifications required; VII. Establish procedures to receive and answer questions and complaints of the data owners in connection with their personal data; VIII. Have mechanisms to comply with the privacy policies and programs, as well as sanctions for the breach thereof; IX. Establish measures to secure personal data, i.e., a set of technical and administrative actions to guarantee the compliance with the principles and obligations stated in the Law and the Regulations hereof, or X. Establish measures for the traceability of personal data, i.e., actions, measures and technical procedures to trace personal data during their processing. Article 61(VII): In order to establish and maintain the security of personal data, the data controller must take into account the following actions: (VII) Train personnel who process personal data…
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	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the	*REGULATION* Article 48. Pursuant to Article 14 of the Law, the data controller shall adopt measures to guarantee the due processing, favoring the data owner's interests and the reasonable expectation of privacy. The measures that

which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures? 30.d) Physical security?	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. 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.	may be adopted by the data controller include, indicatively but without limitation thereto, the following: I. Prepare mandatory and enforceable privacy policies and programs within the data controller's organization; II. Implement a training, updating and awareness program for the personnel as regards the obligations in matters of protection of personal data; III. Establish an internal supervision and oversight system, external audits to prove the compliance with privacy policies; IV. Allocate resources to implement privacy programs and policies; V. Implement a procedure to address the risk for the protection of personal data due to the implementation of new products, services, technologies and business models, as well as mitigate them; VI. Periodically review the security policies and programs to determine the modifications required; VII. Establish procedures to receive and answer questions and complaints of the data owners in connection with their personal data; VIII. Have mechanisms to comply with the privacy policies and programs, as well as sanctions for the breach thereof; IX. Establish measures to secure personal data, i.e., a set of technical and administrative actions to guarantee the compliance with the principles and obligations stated in the Law and the Regulations hereof, or X. Establish measures for the traceability of personal data, i.e., actions, measures and technical

		procedures to trace personal data during their processing. Article 61: In order to guarantee the security of personal data, the data controller shall consider the following actions: I. Prepare an inventory of personal data and of processing systems; II. Determine the functions and obligations of the persons who process personal data; III. Have a risk analysis of personal data that entails identifying dangers and estimating the risks to personal data; IV. Establish the security measures applicable to personal data and identify those implemented effectively; V. Analyze the gap/divide that consists of the difference between the existing security measures and those missing, necessary for the protection of personal data; VI. Prepare a work plan for the implementation of the missing security measures arising from the analysis of the gap/divide; VII. Carry out reviews and/or audits; VIII. Train the personnel who will carry out the processing, and IX. Keep a register of storage means of personal data.
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant answers **NO**, the	*REGULATION* Article 105: Pursuant to Article 25 of the Law, cancellation implies the cessation of the processing of personal data by the data controller, starting from its blockage and its subsequent deletion.

	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.	Article 107 (IV): If the cancellation is warranted, and without prejudice to the provisions of Article 32 of the Law, the data controller shall: (IV) IV. After the blockage period, carry out the suppression using the security measures previously established by the data controller.
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	*REGULATION* Article 61(iii): In order to guarantee the security of personal data, the data controller shall consider the following actions…(iii) Have a risk analysis of personal data that entails identifying dangers and estimating the risks to personal data Article 66: In case of a violation to the personal data, the data controller shall analyze the causes for it and implement the corrective, preventive and improvement actions to adapt the corresponding security measures, in order to avoid the repetition of the violation.
33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	*REGULATION* Article 61(v): In order to guarantee the security of personal data, the data controller shall consider the following actions…(v) Analyze the gap/divide that consists of the difference between the existing security measures and those missing, necessary for the protection of personal data.
34. Do you use risk assessments or third-party certifications? Describe below.	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	*REGULATION* Article 61(vii): In order to guarantee the security of personal data, the data controller shall consider the following actions…(vii) Carry out reviews and/or audits.

	recommendations made in the audits are implemented.	
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?	The Accountability Agent must verify that the Applicant 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.	*REGULATION* Article 47: Pursuant to Articles 6 and 14 of the Law, the data controller has the obligation to safeguard and respond for the processing of the personal data he guards or collects, or for those he communicated to a data processor whether the latter is in Mexican territory or not. To comply with this obligation, the data controller may use standards, international best practices, corporate policies, self-regulation schemes or any other mechanism he deems appropriate for said purposes. Article 50 (III): The data processor shall have the following obligations with respect to the processing carried out on behalf of the data controller: (III) Implement the security measures required by the Law, these Regulations, and other applicable laws and regulations… Article 51: The relationship between the data controller and data processor must be established by contract or other legal instrument decided upon by the data controller and that permits its existence, scope, and contents to be proven.

ACCESS AND CORRECTION

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**JOP Finding**
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable	*LAW* Article 23: Data owners will have the right to access their personal data held by the data controller as well as to be informed of the privacy notice to which processing is subject. *REGULATION* Article 101: Pursuant to Article 23 of the Law, the data owner has the right to obtain his personal data from the data controller, as well as information regarding the conditions and general features of the processing**.**

	qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)? 37.e) Do you charge a fee for	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	*LAW* Article 23: Data owners will have the right to access their personal data held by the data controller as well as to be informed of the privacy notice to which processing is subject. Article 29: The access, rectification, cancellation or objection request must include the following: i. The data owner's name and address or other means to notify him of the response to his request; ii. Documents establishing the identity or, where appropriate, legal representation of the data owner; iii. A clear and precise description of the personal data with regard to which the data owner seeks to exercise any of the abovementioned rights; iv. Any other item or document that facilitates locating the personal data. Article 30: All data controllers must designate a personal data person or department who will process requests from data owners for the exercise of the rights referred to in this Law. In addition, data controllers will promote protection of personal data within their organizations. Article 31: In the case of requests for rectification of personal data, the data owner must indicate, in addition to that which is specified in the preceding article of this Law, the changes to be made, and provide documentation supporting the request.

providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.		Article 32: The data controller will notify the data owner, within a maximum of twenty days counted from the date of receipt of the request for access, rectification, cancellation or objection, of the determination made, so that, where appropriate, same will become effective within fifteen days from the date on which the notice is provided. For personal data access requests, delivery will be made upon proof of identity of the requesting party or legal representative. The aforementioned time periods may be extended a single time by a period of equal length, provided that such action is justified by the circumstances of the case. Article 34: … In all of the aforementioned cases, the data controller must notify the data owner, or, as appropriate, his legal representative, of its decision and the reason for such decision, within the periods established for such purposes, via the same means by which the request was made, attaching, where appropriate, any relevant evidence. Article 35: The action of providing personal data will be free, and the data owner must only pay justified expenses of shipping or the cost of copying or providing data in other formats. This right will be exercised by the data owner free of charge, upon proof of his identity to the data controller. However, if the same person repeats his request within a period of twelve months, costs will not be greater than three days of the General Current Minimum Wage in Mexico City, unless there are material changes to the privacy notice that prompt new queries. The data owner may file a data protection request due to the response received or lack of response from the data controller, in accordance with the provisions of the following Chapter. *REGULATION*

		Article 90: For the exercise of the ARCO rights, the data owner or his representative may submit a request before the data controller in accordance with the means established in the privacy notice. For this purpose, the data controller may make the remote or local means available to the data owner or other means he deems appropriate. Also, the data controller may establish formats, systems or other simplified means to facilitate the exercise of the data owner's ARCO rights, which shall be informed in the privacy notice. Article 93: The exercise of the ARCO rights shall be easy and free. The data owner shall only pay for postage and handling, reproduction and if applicable, document certification, with the exception of what is stated in Article 35, second paragraph of the Law. The reproduction costs may not exceed the recovery costs of the corresponding material. The data controller may not establish any service or means at any cost as the only way to present a request for the exercise of the ARCO rights. Article 98: In all cases, the data controller shall answer the ARCO rights requests he receives, regardless he has the data owner's personal data in his databases or not, in accordance with the periods stated in Article 32 of the Law. The answer to the data owner shall exclusively refer to the personal data specifically indicated in the corresponding request, and shall be presented in a format that has to be legible, understandable and of easy access. In the case of the use of codes, acronyms or keys, the corresponding meanings shall be provided. Article 100: If the data controller refuses the exercise of

		any of the ARCO rights, he shall justify his answer and inform the data owner of his rights to request the beginning of the procedure for the protection of rights before the Institute. Article 101: Pursuant to Article 23 of the Law, the data owner has the right to obtain his personal data from the data controller, as well as information regarding the conditions and general features of the processing. Article 103: Pursuant to Article 24 of the Law, the data owner may request at any time to the data controller, to correct his personal data if it is inaccurate or incomplete. Article 106: The data owner may at any time request to the data controller, the cancelation of his personal data when he considers they are not being processed in accordance with the principles and duties set forth in the Law and the regulations hereof. Depending on the request, the cancellation will apply to all personal data of the data owner contained in a database or only to a certain part of them.
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner?	Where the Applicant answers **YES** to questions 38.a, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where	*LAW* Article 24: The data owner will have the right to rectify data if it is inaccurate or incomplete. Article 25: The data owner will at all times have the right to cancel his personal data. Article 32: The data controller will notify the data owner, within a maximum of twenty days counted from the date of receipt of the request for access, rectification, cancellation or objection, of the determination made, so that, where

Provide a description in the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 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?	appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	appropriate, same will become effective within fifteen days from the date on which the notice is provided. For personal data access requests, delivery will be made upon proof of identity of the requesting party or legal representative. The aforementioned time periods may be extended a single time by a period of equal length, provided that such action is justified by the circumstances of the case. Article 34: The data controller may deny access to personal data or refuse the rectification, cancellation or objection with relation thereto in the following cases: I. Where the requesting party is not the subject of the personal data, or the legal representative is not duly accredited for such purposes; II. Where the requesting party's personal data is not found in the data controller's database; III. Where the rights of a third party are adversely affected; IV. Where there is any legal impediment, or decision of a competent authority, restricting access to the personal data or not allowing the rectification, cancellation or objection with relation thereto, and V. Where the rectification, cancellation or objection has been previously performed. The refusal referred to in this article may be partial, in which case the data controller will carry out the access, rectification, cancellation or objection requested by the data owner. In all of the aforementioned cases, the data controller must notify the data owner, or, as appropriate, his legal representative, of its decision and the reason for such decision, within the periods established for such purposes, via the same means by which the request was

		made, attaching, where appropriate, any relevant evidence. Article 35: The action of providing personal data will be free, and the data owner must only pay justified expenses of shipping or the cost of copying or providing data in other formats. This right will be exercised by the data owner free of charge, upon proof of his identity to the data controller. However, if the same person repeats his request within a period of twelve months, costs will not be greater than three days of the General Current Minimum Wage in Mexico City, unless there are material changes to the privacy notice that prompt new queries. The data owner may file a data protection request due to the response received or lack of response from the data controller, in accordance with the provisions of the following Chapter. *REGULATION* Article 24: The privacy notice shall be simple, with the necessary information, written in clear and understandable language and with a structure and design that make it easy to understand. Article 90: For the exercise of the ARCO rights, the data owner or his representative may submit a request before the data controller in accordance with the means established in the privacy notice. For this purpose, the data controller may make the remote or local means available to the data owner or other means he deems appropriate. Also, the data controller may establish formats, systems or other simplified means to facilitate the exercise of the data owner's ARCO rights, which shall be informed in the privacy notice. Article 93: The exercise of the ARCO rights shall be easy

		and free. The data owner shall only pay for postage and handling, reproduction and if applicable, document certification, with the exception of what is stated in Article 35, second paragraph of the Law. The reproduction costs may not exceed the recovery costs of the corresponding material. The data controller may not establish any service or means at any cost as the only way to present a request for the exercise of the ARCO rights. Article 98: In all cases, the data controller shall answer the ARCO rights requests he receives, regardless he has the data owner's personal data in his databases or not, in accordance with the periods stated in Article 32 of the Law. The answer to the data owner shall exclusively refer to the personal data specifically indicated in the corresponding request, and shall be presented in a format that has to be legible, understandable and of easy access. In the case of the use of codes, acronyms or keys, the corresponding meanings shall be provided. Article 100: If the data controller refuses the exercise of any of the ARCO rights, he shall justify his answer and inform the data owner of his rights to request the beginning of the procedure for the protection of rights before the Institute. Article 101: Pursuant to Article 23 of the Law, the data owner has the right to obtain his personal data from the data controller, as well as information regarding the conditions and general features of the processing. Article 103: Pursuant to Article 24 of the Law, the data owner may request at any time to the data controller, to correct his personal data if it is inaccurate or incomplete.

		Article 106: T he data owner may at any time request to the data controller, the cancelation of his personal data when he considers they are not being processed in accordance with the principles and duties set forth in the Law and the regulations hereof. Depending on the request, the cancellation will apply to all personal data of the data owner contained in a database or only to a certain part of them.

ACCOUNTABILITY

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**JOP Finding**
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations ____ • Compliance with self-regulatory applicant code and/or rules ____ • Other (describe) ____	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	*LAW* Article 6: Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law. Article 14: The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. The data controller must take all necessary and sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship. Article 36: Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data. *REGULATION* Article 47: Pursuant to Articles 6 and 14 of the Law, the data controller has the obligation to safeguard and respond for the processing of the personal data he guards or collects,

		or for those he communicated to a data processor whether the latter is in Mexican territory or not. To comply with this obligation, the data controller may use standards, international best practices, corporate policies, self-regulation schemes or any other mechanism he deems appropriate for said purposes. Article 48: Pursuant to Article 14 of the Law, the data controller shall adopt measures to guarantee the due processing, favoring the data owner's interests and the reasonable expectation of privacy. The measures that may be adopted by the data controller include, indicatively but without limitation thereto, the following: I. Prepare mandatory and enforceable privacy policies and programs within the data controller's organization; II. Implement a training, updating and awareness program for the personnel as regards the obligations in matters of protection of personal data; III. Establish an internal supervision and oversight system, external audits to prove the compliance with privacy policies; IV. Allocate resources to implement privacy programs and policies; V. Implement a procedure to address the risk for the protection of personal data due to the implementation of new products, services, technologies and business models, as well as mitigate them; VI. Periodically review the security policies and programs to determine the modifications required; VII. Establish procedures to receive and answer questions and complaints of the data owners in connection with their personal data;

		VIII. Have mechanisms to comply with the privacy policies and programs, as well as sanctions for the breach thereof; IX. Establish measures to secure personal data, i.e., a set of technical and administrative actions to guarantee the compliance with the principles and obligations stated in the Law and the Regulations hereof, or X. Establish measures for the traceability of personal data, i.e., actions, measures and technical procedures to trace personal data during their processing. Article 50. The data processor shall have the following obligations as regards the processing he carries out as instructed by the data controller: I. Only process personal data according to the data controller's instructions; II. Refrain from processing personal data for purposes different from those informed by the data controller; III. Implement security measures in accordance with the Law, the Regulations and other applicable provisions; IV. Maintain confidentiality as regards processed personal data; V. Delete the personal data processed once the legal relationship with the data controller is terminated or as informed by the data controller, provided there is no legal provision requiring the retention of personal data, and VI. Refrain from transferring personal data except when the data controller so determines it, when the communication derives from an outsourcing or

		when the competent authority so requires it. The agreements between the data controller and the data processor related to the processing shall be in accordance with the corresponding privacy notice. Article 51: The relationship between the data controller and the data processor shall be established by an agreement or other legal instrument determined by the data controller to accredit its existence, scope and content. Article 54: Any outsourcing services by the data processor that entail the processing of personal data, shall be authorized by the data controller and will be carried out on his behalf. After obtaining authorization the data processor must formalize an agreement or other legal instrument with the outsourcer, in order to accredit its existence, scope and content. The outsourced individual or legal entity shall assume the same obligations established for the data processor under the Law, the Regulations hereof and other applicable provisions. The obligation to prove that the outsourcing was done with the data controller's authorization shall fall on the data processor. Article 55: When the agreement or legal instruments used to formalize the relationship between the data controller and the data processor provide for that the latter may outsource services, the authorization referred to in the foregoing article shall be understood as granted through these instruments. If the outsourcing was not provided for in the agreement or the legal instruments referred to in the foregoing paragraph, the data processor shall obtain the corresponding authorization from the data controller prior to the outsourcing. In both cases, the foregoing article shall be

		observed. Article 72: The recipient of personal data shall abide by the Law and the Regulations hereof acting as data controller, and shall process personal data in accordance with the privacy notice informed by the transferor data controller. Article 73. The transfers shall be formalized through a mechanism showing that the transferor data controller informed the recipient data controller of the conditions in which the data owner consented to the processing of his personal data. Article 74: Without detriment to Article 37 of the Law, international transfers of personal data may be possible when the recipient of the personal data takes on the same obligations as the data controller who transferred the personal data. Article 75: For this purpose, the data controller who transfers the personal data may use agreements or other legal instruments providing for the same obligations as the data controller who transferred the personal data, as well as the conditions in which the data owner consented to the processing of his personal data.
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy	*LAW* Article 30: All data controllers must designate a personal data person or department who will process requests from data owners for the exercise of the rights referred to in this Law. In addition, data controllers will promote protection of personal data within their organizations. *REGULATION* Article 48: Pursuant to Article 14 of the Law, the data

	Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	controller shall adopt measures to guarantee the due processing, favoring the data owner's interests and the reasonable expectation of privacy. The measures that may be adopted by the data controller include, indicatively but without limitation thereto, the following: I. Prepare mandatory and enforceable privacy policies and programs within the data controller's organization; II. Implement a training, updating and awareness program for the personnel as regards the obligations in matters of protection of personal data; ; III. Establish an internal supervision and oversight system, external audits to prove the compliance with privacy policies; IV. Allocate resources to implement privacy programs and policies; V. Implement a procedure to address the risk for the protection of personal data due to the implementation of new products, services, technologies and business models, as well as mitigate them; VI. Periodically review the security policies and programs to determine the modifications required; VII. Establish procedures to receive and answer questions and complaints of the data owners in connection with their personal data; VIII. Have mechanisms to comply with the privacy policies and programs, as well as sanctions for the breach thereof; IX. Establish measures to secure personal data, i.e., a set of technical and administrative actions to guarantee the compliance with the principles and obligations stated in the Law and the Regulations hereof, or

		X. Establish measures for the traceability of personal data, i.e., actions, measures and technical procedures to trace personal data during their processing.
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	*LAW* Article 30: All data controllers must designate a personal data person or department who will process requests from data owners for the exercise of the rights referred to in this Law. In addition, data controllers will promote protection of personal data within their organizations.
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their	*LAW* Article 32: The data controller will notify the data owner, within a maximum of twenty days counted from the date of receipt of the request for access, rectification, cancellation

	complaints. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	or objection, of the determination made, so that, where appropriate, same will become effective within fifteen days from the date on which the notice is provided. For personal data access requests, delivery will be made upon proof of identity of the requesting party or legal representative
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	*LAW* Article 32: The data controller will notify the data owner, within a maximum of twenty days counted from the date of receipt of the request for access, rectification, cancellation or objection, of the determination made, so that, where appropriate, same will become effective within fifteen days from the date on which the notice is provided. For personal data access requests, delivery will be made upon proof of identity of the requesting party or legal representative. *REGULATION* Article 100: If the data controller refuses the exercise of any of the ARCO rights, he shall justify his answer and inform the data owner of his rights to request the beginning of the procedure for the protection of rights before the Institute.
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant 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. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the	*REGULATION* Article 48: Pursuant to Article 14 of the Law, the data controller shall adopt measures to guarantee the due processing, favoring the data owner's interests and the reasonable expectation of privacy. The measures that may be adopted by the data controller include, indicatively but without limitation thereto, the following: I. Prepare mandatory and enforceable privacy policies and programs within the data controller's organization; II. Implement a training, updating and awareness program for the personnel as regards the obligations

	existence of such procedures is required for compliance with this principle.	in matters of protection of personal data; III. Establish an internal supervision and oversight system, external audits to prove the compliance with privacy policies; IV. Allocate resources to implement privacy programs and policies; V. Implement a procedure to address the risk for the protection of personal data due to the implementation of new products, services, technologies and business models, as well as mitigate them; VI. Periodically review the security policies and programs to determine the modifications required; VII. Establish procedures to receive and answer questions and complaints of the data owners in connection with their personal data; VIII. Have mechanisms to comply with the privacy policies and programs, as well as sanctions for the breach thereof; IX. Establish measures to secure personal data, i.e., a set of technical and administrative actions to guarantee the compliance with the principles and obligations stated in the Law and the Regulations hereof, or Establish measures for the traceability of personal data, i.e., actions, measures and technical procedures to trace personal data during their processing.
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure	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	*LAW* Article 14: The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data

of personal information?	information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	controller. The data controller must take all necessary and sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship. Article 10(I): Consent for processing of personal data will not be necessary where:…(I) Any Law so provides… Article 34 (I), (V), (VI): Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases:…(I). Where the transfer is pursuant to a Law or Treaty to which Mexico is party;…(V) Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice; (VI.) Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding…
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? • Internal guidelines or policies _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____ • Compliance with self-	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	*LAW* Article 14: The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. The data controller must take all necessary and sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship. Article 36: Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his

regulatory applicant code and/or rules _____ • Other (describe) _____		data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data. *REGULATION* Article 47: Pursuant to Articles 6 and 14 of the Law, the data controller has the obligation to safeguard and respond for the processing of the personal data he guards or collects, or for those he communicated to a data processor whether the latter is in Mexican territory or not. To comply with this obligation, the data controller may use standards, international best practices, corporate policies, self-regulation schemes or any other mechanism he deems appropriate for said purposes. Article 50: The data processor shall have the following obligations as regards the processing he carries out as instructed by the data controller: VII. Only process personal data according to the data controller's instructions; VIII. Refrain from processing personal data for purposes different from those informed by the data controller; IX. Implement security measures in accordance with the Law, the Regulations and other applicable provisions; X. Maintain confidentiality as regards processed personal data; XI. Delete the personal data processed once the legal relationship with the data controller is terminated or as informed by the data controller, provided there is no legal provision requiring the retention of personal data, and XII. Refrain from transferring personal data except when

		the data controller so determines it, when the communication derives from an outsourcing or when the competent authority so requires it. The agreements between the data controller and the data processor related to the processing shall be in accordance with the corresponding privacy notice. Article 51: The relationship between the data controller and the data processor shall be established by an agreement or other legal instrument determined by the data controller to accredit its existence, scope and content. Article 54: Any outsourcing services by the data processor that entail the processing of personal data, shall be authorized by the data controller and will be carried out on his behalf. After obtaining authorization the data processor must formalize an agreement or other legal instrument with the outsourcer, in order to accredit its existence, scope and content. The outsourced individual or legal entity shall assume the same obligations established for the data processor under the Law, the Regulations hereof and other applicable provisions. The obligation to prove that the outsourcing was done with the data controller's authorization shall fall on the data processor. Article 55: When the agreement or legal instruments used to formalize the relationship between the data controller and the data processor provide for that the latter may outsource services, the authorization referred to in the foregoing article shall be understood as granted through these instruments. If the outsourcing was not provided for in the agreement or the legal instruments referred to in the foregoing paragraph, the data processor shall obtain the

		corresponding authorization from the data controller prior to the outsourcing. In both cases, the foregoing article shall be observed. Article 72: The recipient of personal data shall abide by the Law and the Regulations hereof acting as data controller, and shall process personal data in accordance with the privacy notice informed by the transferor data controller. Article 73. The transfers shall be formalized through a mechanism showing that the transferor data controller informed the recipient data controller of the conditions in which the data owner consented to the processing of his personal data. Article 74: Without detriment to Article 37 of the Law, international transfers of personal data may be possible when the recipient of the personal data takes on the same obligations as the data controller who transferred the personal data. Article 75: For this purpose, the data controller who transfers the personal data may use agreements or other legal instruments providing for the same obligations as the data controller who transferred the personal data, as well as the conditions in which the data owner consented to the processing of his personal data.
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your APEC-compliant privacy policies	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	*LAW* Article 14: The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. The data controller must take all necessary and

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 the case of a breach of the personal information of the Applicant's customers? • Other (describe) _____		sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship. Article 36: Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data. *REGULATION* Article 47: Pursuant to Articles 6 and 14 of the Law, the data controller has the obligation to safeguard and respond for the processing of the personal data he guards or collects, or for those he communicated to a data processor whether the latter is in Mexican territory or not. To comply with this obligation, the data controller may use standards, international best practices, corporate policies, self-regulation schemes or any other mechanism he deems appropriate for said purposes. Article 50: The data processor shall have the following obligations as regards the processing he carries out as instructed by the data controller: I. Only process personal data according to the data controller's instructions; II. Refrain from processing personal data for purposes different from those informed by the data controller;

		III. Implement security measures in accordance with the Law, the Regulations and other applicable provisions; IV. Maintain confidentiality as regards processed personal data; V. Delete the personal data processed once the legal relationship with the data controller is terminated or as informed by the data controller, provided there is no legal provision requiring the retention of personal data, and VI. Refrain from transferring personal data except when the data controller so determines it, when the communication derives from an outsourcing or when the competent authority so requires it. The agreements between the data controller and the data processor related to the processing shall be in accordance with the corresponding privacy notice. Article 51: The relationship between the data controller and the data processor shall be established by an agreement or other legal instrument determined by the data controller to accredit its existence, scope and content. Article 54: Any outsourcing services by the data processor that entail the processing of personal data, shall be authorized by the data controller and will be carried out on his behalf. After obtaining authorization the data processor must formalize an agreement or other legal instrument with the outsourcer, in order to accredit its existence, scope and content. The outsourced individual or legal entity shall assume the same obligations established for the data processor under the Law, the Regulations hereof and other applicable provisions. The obligation to prove

		that the outsourcing was done with the data controller's authorization shall fall on the data processor. Article 55: When the agreement or legal instruments used to formalize the relationship between the data controller and the data processor provide for that the latter may outsource services, the authorization referred to in the foregoing article shall be understood as granted through these instruments. If the outsourcing was not provided for in the agreement or the legal instruments referred to in the foregoing paragraph, the data processor shall obtain the corresponding authorization from the data controller prior to the outsourcing. In both cases, the foregoing article shall be observed. Article 72: The recipient of personal data shall abide by the Law and the Regulations hereof acting as data controller, and shall process personal data in accordance with the privacy notice informed by the transferor data controller. Article 73: The transfers shall be formalized through a mechanism showing that the transferor data controller informed the recipient data controller of the conditions in which the data owner consented to the processing of his personal data. Article 74: Without detriment to Article 37 of the Law, international transfers of personal data may be possible when the recipient of the personal data takes on the same obligations as the data controller who transferred the personal data. Article 75: For this purpose, the data controller who transfers the personal data may use agreements or other

		legal instruments providing for the same obligations as the data controller who transferred the personal data, as well as the conditions in which the data owner consented to the processing of his personal data.
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.	The Accountability Agent must verify the existence of such self-assessments.	*REGULATION* Article 48: Pursuant to Article 14 of the Law, the data controller shall adopt measures to guarantee the due processing, favoring the data owner's interests and the reasonable expectation of privacy. The measures that may be adopted by the data controller include, indicatively but without limitation thereto, the following: I. Prepare mandatory and enforceable privacy policies and programs within the data controller's organization; II. Implement a training, updating and awareness program for the personnel as regards the obligations in matters of protection of personal data; III. Establish an internal supervision and oversight system, external audits to prove the compliance with privacy policies; IV. Allocate resources to implement privacy programs and policies; V. Implement a procedure to address the risk for the protection of personal data due to the implementation of new products, services, technologies and business models, as well as mitigate them; VI. Periodically review the security policies and programs to determine the modifications required; VII. Establish procedures to receive and answer questions and complaints of the data owners in connection with their personal data; VIII. Have mechanisms to comply with the privacy policies and programs, as well as sanctions for the

		breach thereof; IX. Establish measures to secure personal data, i.e., a set of technical and administrative actions to guarantee the compliance with the principles and obligations stated in the Law and the Regulations hereof, or Establish measures for the traceability of personal data, i.e., actions, measures and technical procedures to trace personal data during their processing.
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	*REGULATION* Article 48: Pursuant to Article 14 of the Law, the data controller shall adopt measures to guarantee the due processing, favoring the data owner's interests and the reasonable expectation of privacy. The measures that may be adopted by the data controller include, indicatively but without limitation thereto, the following: I. Prepare mandatory and enforceable privacy policies and programs within the data controller's organization; II. Implement a training, updating and awareness program for the personnel as regards the obligations in matters of protection of personal data; III. Establish an internal supervision and oversight system, external audits to prove the compliance with privacy policies; IV. Allocate resources to implement privacy programs and policies; V. Implement a procedure to address the risk for the protection of personal data due to the implementation of new products, services, technologies and business models, as well as mitigate them; VI. Periodically review the security policies and

		programs to determine the modifications required; VII. Establish procedures to receive and answer questions and complaints of the data owners in connection with their personal data; VIII. Have mechanisms to comply with the privacy policies and programs, as well as sanctions for the breach thereof; IX. Establish measures to secure personal data, i.e., a set of technical and administrative actions to guarantee the compliance with the principles and obligations stated in the Law and the Regulations hereof, or Establish measures for the traceability of personal data, i.e., actions, measures and technical procedures to trace personal data during their processing.
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 APEC CBPRs by the recipient as described above is impractical or impossible?	If **YES**, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	*LAW* Article 10: Consent for processing of personal data will not be necessary where: I. Any Law so provides; II. The data is contained in publicly available sources; III. The personal data is subject to a prior dissociation procedure; IV. It has the purpose of fulfilling obligations under a legal relationship between the data owner and the data controller; V. There is an emergency situation that could potentially harm an individual in his person or property; VI. It is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data owner is unable to give consent in the terms established by the General Health Law and other applicable laws,

		and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or VII. A resolution is issued by a competent authority. Article 37: Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases: I. Where the transfer is pursuant to a Law or Treaty to which Mexico is party; II. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management; III. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies; IV. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party; V. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice; VI. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and VII. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner.