

DOMESTIC LAWS AND REGULATIONS APPLICABLE TO ACCOUNTABILITY AGENT ACTIVITIES

[NARRATIVE DESCRIPTION]

To become an APEC- recognized Accountability Agent, an applicant must complete and sign the Accountability Agent APEC Recognition Application.

This application includes the following documents: (1) the Accountability Agent Recognition Criteria, which set forth the requirements for participation as a Cross-Border Privacy Rules (CBPR) System Accountability Agent, including (i) prohibitions against conflicts of interest; (ii) processes for evaluating, certifying, and monitoring applicants seeking CBPR certification; (iii) a dispute resolution process; and (iv) an enforcement mechanism; (2) the Accountability Agent Recognition Criteria Checklist, requiring an applicant to describe how it meets each of the Recognition Criteria; (3) an APEC CBPR System Program Requirements Map, which requires an Accountability Agent to map its own program requirement to the CBPR program requirements; (4) an Accountability Agent Case Notes document, attesting that the Accountability Agent has a process for releasing case notes as described in the document; and (5) an Accountability Agent Complaint Statistics document, attesting that the Accountability Agent has a process for releasing complaint statistics as described in the document. By signing and submitting the Recognition Application, an applicant represents that the answers contained in the Recognition Application are true. By publicly posting its Recognition Application, an APEC- recognized Accountability Agent further represents that the answers contained in the document are true.

In the Mexican case, the local law provides specific rules that must be met in addition to the provisions of the preceding paragraph by certifiers, which is an equivalent figure to the Accountability Agents (AA) in the APEC CBPRs System, because both certify private individuals or legal entities that carry out a due processing of personal data and who voluntarily request such certification.

Given that in Mexico there are specific rules to become a certifier, anyone who wants to apply to be an AA recognized by APEC and operate in Mexico, has to meet the Mexican regulations for certification prior to seeking recognition as AA in the APEC CBPRs System.

*Under Mexican law, Article 44 of the Federal Law on Protection of Personal Data held by Private Parties¹ (LFPDPPP in Spanish) provides that persons or entities may agree on binding self-regulatory schemes on the subject matter, in addition to the requirements of this Law. Such schemes can be translated, among others, in the certification for the protection of personal data. Besides, **Chapter VI Binding Self-Regulation** of the Regulations to the LFPDPPP provides that the binding self-regulatory schemes may include certification of those responsible for the protection of personal data. In the event that the data controller decides to undergo a certification procedure, it shall be granted by a certifier different from the data controller in accordance with the parameters that for such purpose may develop the Ministry of Economy (SE), with the support of the Federal Institute of Access to*

¹ http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010. Also, the unofficial English version of the standard can be found at the following link: https://www.privacyassociation.org/media/pdf/knowledge_center/Mexico_Federal_Data_Protection_Act_July2010.pdf

Information and Data Protection (IFAI). Furthermore, the Regulations to the LFPDPPP² note that the main function of the certifiers is to certify the privacy policies, programs and procedures to which data controller parties voluntarily adhere and that ensure proper treatment of the data and the adoption and maintenance of security measures. This ensures the independence and impartiality in granting certificates as well as the compliance with the requirements and criteria set forth in the foregoing parameters. Likewise, the Regulations to the LFPDPPP provide that the abovementioned parameters shall include mechanisms to accredit and revoke the certifying individuals or corporations.

Consistent with the above, in accordance with Article 43, section V of the LFPDPPP, the Ministry of Economy has the authority to state, along with IFAI, the parameters required for the correct development of self-regulatory mechanisms and measures as referred to in Article 44 of said Law, including certification for the protection of personal data. Said parameters have not yet been officially issued; however, on August 15 of this year, the **draft of the Agreement to release the parameters for the proper development of the binding self-regulatory schemes set forth in Article 44 of the Federal Law on Protection of Personal Data Held by Private Parties (Draft of Self-Regulatory Parameters)**, was released for public consultation on the official website of the Federal Commission for Regulatory Improvement (COFEMER) with the intention of receiving feedback from the constituents that may be interested on the subject.³

Chapter V of the Draft of Self-Regulatory Parameters, entitled **About the certification system for the protection of personal data**, develops the aspects and rules governing the Certification System for the protection of personal data in accordance with the provisions in Articles 83, 84 and 85 of the Rules of the Law referred to above. This system is developed in four levels: (1) The IFAI, that authorizes Accrediting Entities, (2) the Accrediting Entities, that are in charge of the accreditation of certifiers, (3) The Certifiers who certify the data controller or the data processors who can meet certain standards in the treatment of personal data, and (4) the data controller or the data processor who want to be certified in the area of personal data.

In this sense, Mexico may nominate and submit to the ECSG, DPS and JOP the relevant application and documentation of those wishing to be recognized as AA in the APEC CBPRs System, once they have been accredited certifiers under framework of the Self-Regulatory Parameters. This accreditation must be made by any Accrediting Entity authorized by IFAI, the authority responsible for monitoring the due processing of personal data in Mexico, according to the LFPDPPP and the **Federal Law of Transparency and Access to Public Government Information (LFTAIPG in Spanish)**. In case the candidate is not accredited as Certifier, there would be a cause for Mexico to reject the applicant's request to be recognized as AA in APEC.⁴

In connection with the certification, the Draft of Self-Regulatory Parameters, **Section IV Of certifiers and certificates**, sets forth the functions, duties and operational criteria that must be met by Certifiers as well as the requirements that an Accrediting Entity should assess to accredit a Certifier. Among those requirements, it is stressed that the Certifier must: (1) Provide identification and location data; (2) Detail the services it intends to provide, the procedures used and the conditions for granting, maintaining, extending, reducing, suspending, restoring and revoking the certification of those data controllers or data processors; (3) Have the financial, technological structure, and staff

² Articles 83, 84 y 85 of the Data Protection Law Secondary Regulations:

<http://www.ordenjuridico.gob.mx/Documentos/Federal/wo66858.doc>

³ http://207.248.177.30/regulaciones/scd_expediente_3.asp?ID=03/2085/150812

⁴ See paragraph 34 of the document: APEC CBPR System - Policies, Rules and Guidelines-, which states that any APEC Economy has the right to refuse the request for an AA to get such recognition.

that is sufficient and is qualified to carry out its activities; (4) Disclose the elements evidencing fairness to the process and document potential conflicts of interest; (5) Outline the issues that ensure the confidentiality of the information they access to; and (6) Describe the management system under which it operates.

The main roles and responsibilities of Certifiers are, among others: (1) Provide, maintain, amend, suspend or revoke the certification of the data controllers or data processors; (2) Comply with the terms and conditions under which the accreditation was granted; (3) Allow the review or verification of their activities by IFAI or the Accrediting Entities; (4) Maintain an ongoing monitoring and surveillance program which can demonstrate at any time that the certified bodies continue to meet the conditions and requirements that formed the basis for the certification; (5) Have procedures resolving specific complaints submitted by the parties affected by their activities and keep records thereof; (6) Submit semiannual reports of their activities and keep them publicly available; (7) Avoid conflicts of interest and act with impartiality, independence and integrity; (8) Operate under a management system; and (9) Constantly update the Accrediting Entity with regards to certificates they issue.

*Furthermore, the Draft of Self-Regulatory Parameters, **Section III Of the accreditation bodies and the accreditation of certifiers**, sets forth the grounds for suspension and revocation of the accreditation to certifiers, mainly when they fail to comply with certain requirements based on which they were granted the accreditation. When the accreditation is suspended or revoked to a Certifier based on the Mexican regulations, the assumption to also request the suspension of recognition of such certifier as AA before APEC could be updated.*

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

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

- (i) The Economy's ECSG delegation, or appropriate governmental representative, submits to the ECSG Chair a letter indicating its intention to participate and confirming that at least one Privacy Enforcement Authority in that Economy is a participant in the APEC Cross Border Privacy Enforcement Arrangement (CPEA);*
- (ii) The Economy indicates its intention to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2 of the Charter of the JOP;*
- (iii) The Economy's ECSG delegation, or appropriate governmental representative, after consulting with the JOP, submits to the Chair of the ECSG an explanation of how the CBPR System program requirements may be enforced in that Economy; and*
- (iv) The JOP submits to the Chair of the ECSG a report as to how the conditions in (i)-(iii) above have been satisfied.*

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

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

Column 1 lists the questions in the intake questionnaire to be answered by an applicant organization when seeking CBPR certification. Column 2 lists the assessment criteria to be used by an APEC-recognized Accountability Agent when verifying the answers provided in Column 1. Column 3 is for use by the Economy's ECSG delegation or appropriate governmental representative when explaining the enforceability of an applicant organization's answers in Column 1. An economy's relevant privacy enforcement authorities should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements. Additional documentation to assist in these explanations may be submitted as necessary. This document is to be read consistently with the qualifications to the provision of notice, the provision of choice mechanisms, and the provision of access and correction mechanisms found in the CBPR Intake Questionnaire.

NOTICE.....	5
COLLECTION LIMITATION.....	11
USES OF PERSONAL INFORMNATION.....	13
CHOICE.....	17
INTEGRITY OF PERSONAL INFORMATION	23
SECURITY SAFEGUARDS	26
ACCESS AND CORRECTION	32
ACCOUNTABILITY.....	36
GENERAL	36
MAINTAINING ACCOUNTABILITY WHEN PERSONAL INFORMATION IS TRANSFERRED	39

NOTICE

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

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
<p>1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.</p>	<p>If YES, the Accountability Agent must verify that the Applicant’s privacy practices and policy (or other privacy statement) include the following characteristics:</p> <ul style="list-style-type: none"> • Available on the Applicant’s Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline. • States an effective date of Privacy Statement publication. <p>Where Applicant answers NO to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies</p>	<ul style="list-style-type: none"> • Articles 3, 8, 15, 16, 17, 33 and 36 of the Federal Law on Protection of Personal Data held by Private Parties (Law) describe the main elements that apply to Privacy Notice, what does it mean, what characteristics it must have, how shall it be implemented and when depending on how the personal data was obtained. Article 36 states the clause the Privacy Notice shall have in order for the data owner to accept transferences in case it is required. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 14, 23-29, 30, 40, 41, 42, 68, 90 and 102 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties (Regulations) describe that under the principle of information, there are many elements to take into account according to the Regulations. They set forth the characteristics, diffusion means, elements, content for Privacy Notice in a limited space, among others. These articles specify that the Privacy Notice must contain, among other elements: the purposes of the treatment (lawful treatments), the distinct purposes for collecting personal data (primary

	<p>an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>purposes – derived from the relationship between the data controller and the data owner- or secondary purposes), report if transferences are made, the ways to obtain different types of consent for those transferences, if consent is needed and the means for data subjects to exercise their rights.</p>
<p>1.a) Does this privacy statement describe how personal information is collected?</p>	<p>If YES, the Accountability Agent must verify that:</p> <ul style="list-style-type: none"> • The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. • the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. <p>If NO, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Articles 3, 8, 15, 16, 17, 33 and 36 of the Federal Law on Protection of Personal Data held by Private Parties (Law) describe the main elements that apply to Privacy Notice, what does it mean, what characteristics it must have, how shall it be implemented and when depending on how the personal data was obtained. Article 36 states the clause the Privacy Notice shall have in order for the data owner to accept transferences in case it is required. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 14, 23-29, 30, 40, 41, 42, 68, 90 and 102 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties (Regulations) describe that under the principle of information, there are many elements to take into account according to the Regulations. They set forth the characteristics, diffusion means, elements, content for Privacy Notice in a limited space, among others. These articles specify that the Privacy Notice must contain, among other elements: the purposes of the treatment (lawful treatments), the distinct purposes for collecting personal data (primary purposes – derived from the relationship between the data controller and the data owner- or secondary purposes), report if transferences are made, the ways to

		<p>obtain different types of consent for those transferences, if consent is needed and the means for data subjects to exercise their rights.</p>
<p>1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides notice to individuals of the purpose for which personal information is being collected.</p> <p>Where the Applicant answers NO and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<ul style="list-style-type: none"> • Articles 3, 8, 15, 16, 17, 33 and 36 of the Federal Law on Protection of Personal Data held by Private Parties (Law) describe the main elements that apply to Privacy Notice, what does it mean, what characteristics it must have, how shall it be implemented and when depending on how the personal data was obtained. Article 36 states the clause the Privacy Notice shall have in order for the data owner to accept transferences in case it is required. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 14, 23-29, 30, 40, 41, 42, 68, 90 and 102 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties (Regulations) describe that under the principle of information, there are many elements to take into account according to the Regulations. They set forth the characteristics, diffusion means, elements, content for Privacy Notice in a limited space, among others. These articles specify that the Privacy Notice must contain, among other elements: the purposes of the treatment (lawful treatments), the distinct purposes for collecting personal data (primary purposes – derived from the relationship between the data controller and the data owner- or secondary purposes), report if transferences are made, the ways to obtain different types of consent for those transferences, if consent is needed and the means for data subjects to

		exercise their rights.
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, <u>identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available.</u></p> <p>Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<ul style="list-style-type: none"> • Articles 3, 8, 15, 16, 17, 33 and 36 of the Federal Law on Protection of Personal Data held by Private Parties (Law) describe the main elements that apply to Privacy Notice, what does it mean, what characteristics it must have, how shall it be implemented and when depending on how the personal data was obtained. Article 36 states the clause the Privacy Notice shall have in order for the data owner to accept transferences in case it is required. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 14, 23-29, 30, 40, 41, 42, 68, 90 and 102 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties (Regulations) describe that under the principle of information, there are many elements to take into account according to the Regulations. They set forth the characteristics, diffusion means, elements, content for Privacy Notice in a limited space, among others. These articles specify that the Privacy Notice must contain, among other elements: the purposes of the treatment (lawful treatments), the distinct purposes for collecting personal data (primary purposes – derived from the relationship between the data controller and the data owner- or secondary purposes), report if transferences are made, the ways to obtain different types of consent for those transferences, if consent is needed and the means for data subjects to exercise their rights.
1.d) Does this privacy	Where the Applicant answers YES , the	<ul style="list-style-type: none"> • Articles 3, 8, 15, 16, 17, 33 and 36 of the Federal Law

<p>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.</p>	<p>Accountability Agent must verify that the Applicant provides name, address and a functional e-mail address.</p> <p>Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant 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.</p>	<p>on Protection of Personal Data held by Private Parties (Law) describe the main elements that apply to Privacy Notice, what does it mean, what characteristics it must have, how shall it be implemented and when depending on how the personal data was obtained. Article 36 states the clause the Privacy Notice shall have in order for the data owner to accept transferences in case it is required.</p> <ul style="list-style-type: none"> • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 14, 23-29, 30, 40, 41, 42, 68, 90 and 102 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties (Regulations) describe that under the principle of information, there are many elements to take into account according to the Regulations. They set forth the characteristics, diffusion means, elements, content for Privacy Notice in a limited space, among others. These articles specify that the Privacy Notice must contain, among other elements: the purposes of the treatment (lawful treatments), the distinct purposes for collecting personal data (primary purposes – derived from the relationship between the data controller and the data owner- or secondary purposes), report if transferences are made, the ways to obtain different types of consent for those transferences, if consent is needed and the means for data subjects to exercise their rights.
<p>1.e) Does this privacy statement provide information regarding the use and disclosure</p>	<p>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</p>	<ul style="list-style-type: none"> • Articles 3, 8, 15, 16, 17, 33 and 36 of the Federal Law on Protection of Personal Data held by Private Parties (Law) describe the main elements that apply to Privacy Notice, what does it mean, what characteristics

<p>of an individual's personal information?</p>	<p>personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>it must have, how shall it be implemented and when depending on how the personal data was obtained. Article 36 states the clause the Privacy Notice shall have in order for the data owner to accept transferences in case it is required.</p> <ul style="list-style-type: none"> • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 14, 23-29, 30, 40, 41, 42, 68, 90 and 102 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties (Regulations) describe that under the principle of information, there are many elements to take into account according to the Regulations. They set forth the characteristics, diffusion means, elements, content for Privacy Notice in a limited space, among others. These articles specify that the Privacy Notice must contain, among other elements: the purposes of the treatment (lawful treatments), the distinct purposes for collecting personal data (primary purposes – derived from the relationship between the data controller and the data owner- or secondary purposes), report if transferences are made, the ways to obtain different types of consent for those transferences, if consent is needed and the means for data subjects to exercise their rights.
<p>1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Privacy Statement includes:</p> <ul style="list-style-type: none"> • The process through which the individual may access his or her personal information (including electronic or traditional non- 	<ul style="list-style-type: none"> • Articles 3, 8, 15, 16, 17, 33 and 36 of the Federal Law on Protection of Personal Data held by Private Parties (Law) describe the main elements that apply to Privacy Notice, what does it mean, what characteristics it must have, how shall it be implemented and when depending on how the personal data was obtained. Article 36 states the clause the Privacy Notice shall

<p>personal information?</p>	<p>electronic means).</p> <ul style="list-style-type: none"> • The process that an individual must follow in order to correct his or her personal information <p>Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant’s typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<p>have in order for the data owner to accept transferences in case it is required.</p> <ul style="list-style-type: none"> • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 14, 23-29, 30, 40, 41, 42, 68, 90 and 102 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties (Regulations) describe that under the principle of information, there are many elements to take into account according to the Regulations. They set forth the characteristics, diffusion means, elements, content for Privacy Notice in a limited space, among others. These articles specify that the Privacy Notice must contain, among other elements: the purposes of the treatment (lawful treatments), the distinct purposes for collecting personal data (primary purposes – derived from the relationship between the data controller and the data owner- or secondary purposes), report if transferences are made, the ways to obtain different types of consent for those transferences, if consent is needed and the means for data subjects to exercise their rights.
<p>2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected <u>and that the notice is reasonably available to individuals.</u></p> <p>Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that</p>	<ul style="list-style-type: none"> • Articles 3, 8, 15, 16, 17, 33 and 36 of the Federal Law on Protection of Personal Data held by Private Parties (Law) describe the main elements that apply to Privacy Notice, what does it mean, what characteristics it must have, how shall it be implemented and when depending on how the personal data was obtained. Article 36 states the clause the Privacy Notice shall have in order for the data owner to accept transferences in case it is required.

<p>being collected?</p>	<p>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.</p>	<ul style="list-style-type: none"> • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 14, 23-29, 30, 40, 41, 42, 68, 90 and 102 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties (Regulations) describe that under the principle of information, there are many elements to take into account according to the Regulations. They set forth the characteristics, diffusion means, elements, content for Privacy Notice in a limited space, among others. These articles specify that the Privacy Notice must contain, among other elements: the purposes of the treatment (lawful treatments), the distinct purposes for collecting personal data (primary purposes – derived from the relationship between the data controller and the data owner- or secondary purposes), report if transferences are made, the ways to obtain different types of consent for those transferences, if consent is needed and the means for data subjects to exercise their rights.
<p>3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant’s website, such as text on a website link from URL, attached documents, pop-up window, or other.</p> <p>Where the Applicant answers NO and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform</p>	<ul style="list-style-type: none"> • Articles 3, 8, 15, 16, 17, 33 and 36 of the Federal Law on Protection of Personal Data held by Private Parties (Law) describe the main elements that apply to Privacy Notice, what does it mean, what characteristics it must have, how shall it be implemented and when depending on how the personal data was obtained. Article 36 states the clause the Privacy Notice shall have in order for the data owner to accept transferences in case it is required. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data,

	<p>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.</p>	<p>which will be imposed when a violation occurs.</p> <ul style="list-style-type: none"> • Articles 14, 23-29, 30, 40, 41, 42, 68, 90 and 102 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties (Regulations) describe that under the principle of information, there are many elements to take into account according to the Regulations. They set forth the characteristics, diffusion means, elements, content for Privacy Notice in a limited space, among others. These articles specify that the Privacy Notice must contain, among other elements: the purposes of the treatment (lawful treatments), the distinct purposes for collecting personal data (primary purposes – derived from the relationship between the data controller and the data owner- or secondary purposes), report if transferences are made, the ways to obtain different types of consent for those transferences, if consent is needed and the means for data subjects to exercise their rights.
<p>4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes.</p> <p>Where the Applicant answers NO and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification</p>	<ul style="list-style-type: none"> • Articles 3, 8, 15, 16, 17, 33 and 36 of the Federal Law on Protection of Personal Data held by Private Parties (Law) describe the main elements that apply to Privacy Notice, what does it mean, what characteristics it must have, how shall it be implemented and when depending on how the personal data was obtained. Article 36 states the clause the Privacy Notice shall have in order for the data owner to accept transferences in case it is required. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 14, 23-29, 30, 40, 41, 42, 68, 90 and 102 of the

	is justified.	<p>Regulations to the Federal Law on Protection of Personal Data held by Private Parties (Regulations) describe that under the principle of information, there are many elements to take into account according to the Regulations. They set forth the characteristics, diffusion means, elements, content for Privacy Notice in a limited space, among others. These articles specify that the Privacy Notice must contain, among other elements: the purposes of the treatment (lawful treatments), the distinct purposes for collecting personal data (primary purposes – derived from the relationship between the data controller and the data owner- or secondary purposes), report if transferences are made, the ways to obtain different types of consent for those transferences, if consent is needed and the means for data subjects to exercise their rights.</p>
--	---------------	---

COLLECTION LIMITATION

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

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
<p>5. How do you obtain personal information:</p> <p>5.a) Directly from the individual?</p> <p>5.b) From third parties collecting on your behalf?</p> <p>5.c) Other. If YES, describe.</p>	<p>The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information.</p> <p>Where the Applicant answers YES to any of these sub-parts, the Accountability Agent must verify the Applicant’s practices in this regard.</p> <p>There should be at least one ‘yes’ answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.</p>	<ul style="list-style-type: none"> • With regard to data collection limitation, Articles 7, 8, 12 and 13 of the Federal Law on Protection of Personal Data held by Private Parties emphasize that data shall be collected in a lawful manner in accordance with the provisions in the Law and the rest of the applicable regulations, and limited to the specific purposes informed at the time of the collection. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 10, 11, 17, 44, 45 and 46 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the obligations to limit the collection of personal data to accomplish the purposes informed in the Privacy Notice. Moreover, the information must be obtained licitly. The consent of the data owner must be collected, unless it is not required by the exceptions previously established.
<p>6. Do you limit your</p>	<p>Where the Applicant answers YES and indicates it only</p>	<ul style="list-style-type: none"> • With regard to data collection limitation, Articles

<p>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?</p>	<p>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:</p> <ul style="list-style-type: none"> • Each type of data collected • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data • An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection <p>Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.</p>	<p>7, 8, 12 and 13 of the Federal Law on Protection of Personal Data held by Private Parties emphasize that data shall be collected in a lawful manner in accordance with the provisions in the Law and the rest of the applicable regulations, and limited to the specific purposes informed at the time of the collection.</p> <ul style="list-style-type: none"> • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 10, 11, 17, 44, 45 and 46 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the obligations to limit the collection of personal data to accomplish the purposes informed in the Privacy Notice. Moreover, the information must be obtained licitly. The consent of the data owner must be collected, unless it is not required by the exceptions previously established.
<p>7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information?</p>	<p>Where the Applicant answers YES, the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception.</p> <p>Where the Applicant Answers NO, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.</p>	<ul style="list-style-type: none"> • With regard to data collection limitation, Articles 7, 8, 12 and 13 of the Federal Law on Protection of Personal Data held by Private Parties emphasize that data shall be collected in a lawful manner in accordance with the provisions in the Law and the rest of the applicable regulations, and limited to the specific purposes informed at the time of the collection. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the

Where YES, describe.		<p>Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs.</p> <ul style="list-style-type: none"> • Articles 10, 11, 17, 44, 45 and 46 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the obligations to limit the collection of personal data to accomplish the purposes informed in the Privacy Notice. Moreover, the information must be obtained licitly. The consent of the data owner must be collected, unless it is not required by the exceptions previously established.
----------------------	--	---

USES OF PERSONAL INFORMATION

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

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
<p>8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes.</p> <p>Where the Applicant Answers NO, the Accountability Agent must consider answers to Question 9 below.</p>	<ul style="list-style-type: none"> • Articles 8, 9, 10, 12, 36 and 37 of the Federal Law on Protection of Personal Data held by Private Parties. All processing of personal data shall be subject to the consent of the data owner; in order to use sensitive information express consent is required by Law. The exemptions to consent are specified in article 10. Article 12 states that the use of personal information shall be limited to the purposes established in the Privacy Notice or to similar purposes. Likewise, articles 36 and 37 state the consent clauses needed for transferences and the transferences that need no consent. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 11-16 and 18-22, 40-43 and Chapter IV (articles 67 – 76) of the Regulations to the

		<p>Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations and the consent must be referred to a determined purpose or purposes settled in the Privacy Notice. They also describe the characteristics of the tacit and expressed consent, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Furthermore, the Regulation states that purposes in the Privacy Notice shall be determined, clear and objective so to avoid confusion. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.</p>
<p>9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below.</p> <p>9.a) Based on express consent of the individual?</p>	<p>Where the Applicant answers NO to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant’s use of the personal information is based on express consent of the individual (9.a), such as:</p> <ul style="list-style-type: none"> • Online at point of collection 	<ul style="list-style-type: none"> • Articles 8, 9, 10, 12, 36 and 37 of the Federal Law on Protection of Personal Data held by Private Parties. All processing of personal data shall be subject to the consent of the data owner; in order to use sensitive information express consent is required by Law. The exemptions to consent are specified in article 10. Article 12 states that the use of personal information shall be limited to the purposes established in the Privacy Notice or to similar purposes. Likewise, articles 36 and 37 state the consent clauses needed for transferences and the

<p>9.b) Compelled by applicable laws?</p>	<ul style="list-style-type: none"> • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below.</p> <p>Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law.</p> <p>Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.</p>	<p>transferences that need no consent.</p> <ul style="list-style-type: none"> • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 11-16 and 18-22, 40-43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations and the consent must be referred to a determined purpose or purposes settled in the Privacy Notice. They also describe the characteristics of the tacit and expressed consent, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Furthermore, the Regulation states that purposes in the Privacy Notice shall be determined, clear and objective so to avoid confusion. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.
<p>10. Do you disclose personal information you collect (whether directly or through the use of third</p>	<p>Where the Applicant answers YES in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such</p>	<ul style="list-style-type: none"> • Articles 8, 9, 10, 12, 36 and 37 of the Federal Law on Protection of Personal Data held by Private Parties. All processing of personal data shall be subject to the consent of the data

<p>parties acting on your behalf) to other personal information controllers? If YES, describe.</p>	<p>disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law.</p> <p>Also, the Accountability Agent must require the Applicant to identify:</p> <ol style="list-style-type: none"> 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). <p>Using the above, the Accountability Agent must verify that the Applicant’s disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.</p>	<p>owner; in order to use sensitive information express consent is required by Law. The exemptions to consent are specified in article 10. Article 12 states that the use of personal information shall be limited to the purposes established in the Privacy Notice or to similar purposes. Likewise, articles 36 and 37 state the consent clauses needed for transferences and the transferences that need no consent.</p> <ul style="list-style-type: none"> • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 11-16 and 18-22, 40-43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations and the consent must be referred to a determined purpose or purposes settled in the Privacy Notice. They also describe the characteristics of the tacit and expressed consent, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Furthermore, the Regulation states that purposes in the Privacy Notice shall be determined, clear and objective so to avoid confusion. Additionally, the
--	---	--

		<p>Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.</p>
<p>11. Do you transfer personal information to personal information processors? If YES, describe.</p>		<ul style="list-style-type: none"> • Articles 8, 9, 10, 12, 36 and 37 of the Federal Law on Protection of Personal Data held by Private Parties. All processing of personal data shall be subject to the consent of the data owner; in order to use sensitive information express consent is required by Law. The exemptions to consent are specified in article 10. Article 12 states that the use of personal information shall be limited to the purposes established in the Privacy Notice or to similar purposes. Likewise, articles 36 and 37 state the consent clauses needed for transferences and the transferences that need no consent. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 11-16 and 18-22, 40-43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations and the consent must be referred to a determined purpose or purposes settled in

		<p>the Privacy Notice. They also describe the characteristics of the tacit and expressed consent, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Furthermore, the Regulation states that purposes in the Privacy Notice shall be determined, clear and objective so to avoid confusion. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.</p>
<p>12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.</p>		<ul style="list-style-type: none"> • Articles 8, 9, 10, 12, 36 and 37 of the Federal Law on Protection of Personal Data held by Private Parties. All processing of personal data shall be subject to the consent of the data owner; in order to use sensitive information express consent is required by Law. The exemptions to consent are specified in article 10. Article 12 states that the use of personal information shall be limited to the purposes established in the Privacy Notice or to similar purposes. Likewise, articles 36 and 37 state the consent clauses needed for transferences and the transferences that need no consent. • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 11-16 and 18-22, 40-43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data

		<p>held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations and the consent must be referred to a determined purpose or purposes settled in the Privacy Notice. They also describe the characteristics of the tacit and expressed consent, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Furthermore, the Regulation states that purposes in the Privacy Notice shall be determined, clear and objective so to avoid confusion. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.</p>
<p>13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances?</p> <p>13.a) Based on express consent of the individual?</p> <p>13.b) Necessary to provide a service or product requested by the individual?</p>	<p>Where applicant answers NO to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes.</p> <p>Where the Applicant answers YES to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail 	<ul style="list-style-type: none"> • Articles 8, 9, 10, 12, 36 and 37 of the Federal Law on Protection of Personal Data held by Private Parties. All processing of personal data shall be subject to the consent of the data owner; in order to use sensitive information express consent is required by Law. The exemptions to consent are specified in article 10. Article 12 states that the use of personal information shall be limited to the purposes established in the Privacy Notice or to similar purposes. Likewise, articles 36 and 37 state the consent clauses needed for transferences and the transferences that need no consent.

<p>13.c) Compelled by applicable laws?</p>	<ul style="list-style-type: none"> • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>Where the Applicant answers YES to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual.</p> <p>Where the Applicant answers YES to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement.</p> <p>Where the Applicant answers NO to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is *required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Articles 63-66 describe the violations to the Law and the penalties that might be enforced by the Federal Institute for Access to Information and Personal Data, which will be imposed when a violation occurs. • Articles 11-16 and 18-22, 40-43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations and the consent must be referred to a determined purpose or purposes settled in the Privacy Notice. They also describe the characteristics of the tacit and expressed consent, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Furthermore, the Regulation states that purposes in the Privacy Notice shall be determined, clear and objective so to avoid confusion. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.
--	--	--

CHOICE

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

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
<p>14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated.</p> <p>Where the Applicant answers NO, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not identify an applicable qualification the Accountability</p>	<ul style="list-style-type: none"> • Articles 8-10, 16, 36, and 37 of the Federal Law on Protection of Personal Data held by Private Parties. Regulating when consent from the data owner is needed, the type of consent needed and the exemption cases. Furthermore, articles 36 and 37 state the consent clauses needed for transferences and the transferences without consent permitted under certain scenarios. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Articles 11-16, 17, 18-22, 40 – 43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain

	<p>Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.</p>	<p>consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations. The consent must be referred to a determined purpose or purposes settle in the Privacy Notice. When personal data is collected directly from the data owner, consent should be obtained before any phase of treatment. They also describe the characteristics of the tacit and expressed consent, their modalities and exceptions, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Moreover articles 40 – 43 explain how to comply with the Principle of Purpose, how to differentiate between purposes, how to oppose a determined purpose and when are different purposes allowed. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.</p>
<p>15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone 	<ul style="list-style-type: none"> • Articles 8-10, 16, 36, and 37 of the Federal Law on Protection of Personal Data held by Private Parties. Regulating when consent from the data owner is needed, the type of consent needed and the exemption cases. Furthermore, articles 36 and 37 state the consent clauses needed for transferences and the transferences without consent permitted under certain scenarios. • Articles 63-66, which describe the acts considered to be violations to the Law and

	<ul style="list-style-type: none"> • Via postal mail, or • Other (in case, specify) <p>The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be 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:]</p> <ul style="list-style-type: none"> • being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service Providers. <p>Where the Applicant answers NO, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified.</p> <p>Where the Applicant answers NO and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.</p>	<p>the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data.</p> <ul style="list-style-type: none"> • Articles 11-16, 17, 18-22, 40 – 43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations. The consent must be referred to a determined purpose or purposes settle in the Privacy Notice. When personal data is collected directly from the data owner, consent should be obtained before any phase of treatment. They also describe the characteristics of the tacit and expressed consent, their modalities and exceptions, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Moreover articles 40 – 43 explain how to comply with the Principle of Purpose, how to differentiate between purposes, how to oppose a determined purpose and when are different purposes allowed. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.
--	---	---

<p>16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. 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:</p> <ul style="list-style-type: none"> • disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant’s choice mechanism is not displayed in a clear and conspicuous manner , or compatible with that for which the information was collected.] <p>Where the Applicant answers NO, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability</p>	<ul style="list-style-type: none"> • Articles 8-10, 16, 36, and 37 of the Federal Law on Protection of Personal Data held by Private Parties. Regulating when consent from the data owner is needed, the type of consent needed and the exemption cases. Furthermore, articles 36 and 37 state the consent clauses needed for transferences and the transferences without consent permitted under certain scenarios. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Articles 11-16, 17, 18-22, 40 – 43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations. The consent must be referred to a determined purpose or purposes settle in the Privacy Notice. When personal data is collected directly from the data owner, consent should be obtained before any phase of treatment. They also describe the characteristics of the tacit and expressed consent, their modalities and exceptions, as well as, the obligations of data controllers
--	---	---

	<p>Agent must verify whether the applicable qualification is justified.</p> <p>Where the Applicant answers NO and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.</p>	<p>and the rights of data owners in order to revoke consent. Moreover articles 40 – 43 explain how to comply with the Principle of Purpose, how to differentiate between purposes, how to oppose a determined purpose and when are different purposes allowed. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.</p>
<p>17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant’s choice mechanism is displayed in a clear and conspicuous manner .</p> <p>Where the Applicant answers NO, or when the Accountability Agent finds that the Applicant’s choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.</p>	<ul style="list-style-type: none"> • Articles 8-10, 16, 36, and 37 of the Federal Law on Protection of Personal Data held by Private Parties. Regulating when consent from the data owner is needed, the type of consent needed and the exemption cases. Furthermore, articles 36 and 37 state the consent clauses needed for transferences and the transferences without consent permitted under certain scenarios. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Articles 11-16, 17, 18-22, 40 – 43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and

		<p>purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations. The consent must be referred to a determined purpose or purposes settle in the Privacy Notice. When personal data is collected directly from the data owner, consent should be obtained before any phase of treatment. They also describe the characteristics of the tacit and expressed consent, their modalities and exceptions, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Moreover articles 40 – 43 explain how to comply with the Principle of Purpose, how to differentiate between purposes, how to oppose a determined purpose and when are different purposes allowed. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.</p>
<p>18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant’s choice mechanism is clearly worded and easily understandable.</p> <p>Where the Applicant answers NO, and/or when the Accountability Agent finds that the Applicant’s choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly</p>	<ul style="list-style-type: none"> • Articles 8-10, 16, 36, and 37 of the Federal Law on Protection of Personal Data held by Private Parties. Regulating when consent from the data owner is needed, the type of consent needed and the exemption cases. Furthermore, articles 36 and 37 state the consent clauses needed for transferences and the transferences without consent permitted under certain scenarios. • Articles 63-66, which describe the acts

	<p>worded and easily understandable in order to comply with this principle.</p>	<p>considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data.</p> <ul style="list-style-type: none"> • Articles 11-16, 17, 18-22, 40 – 43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations. The consent must be referred to a determined purpose or purposes settle in the Privacy Notice. When personal data is collected directly from the data owner, consent should be obtained before any phase of treatment. They also describe the characteristics of the tacit and expressed consent, their modalities and exceptions, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Moreover articles 40 – 43 explain how to comply with the Principle of Purpose, how to differentiate between purposes, how to oppose a determined purpose and when are different purposes allowed. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.
--	---	--

<p>19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant’s choice mechanism is easily accessible and affordable.</p> <p>Where the Applicant answers NO, or when the Accountability Agent finds that the Applicant’s choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.</p>	<ul style="list-style-type: none"> • Articles 8-10, 16, 36, and 37 of the Federal Law on Protection of Personal Data held by Private Parties. Regulating when consent from the data owner is needed, the type of consent needed and the exemption cases. Furthermore, articles 36 and 37 state the consent clauses needed for transferences and the transferences without consent permitted under certain scenarios. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Articles 11-16, 17, 18-22, 40 – 43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations. The consent must be referred to a determined purpose or purposes settle in the Privacy Notice. When personal data is collected directly from the data owner, consent should be obtained before any phase of treatment. They also describe the characteristics of the tacit and expressed consent, their modalities and exceptions, as
--	---	--

		<p>well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Moreover articles 40 – 43 explain how to comply with the Principle of Purpose, how to differentiate between purposes, how to oppose a determined purpose and when are different purposes allowed. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.</p>
<p>20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.</p>	<p>Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored.</p> <p>Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified.</p> <p>Where the Applicant answers NO and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.</p>	<ul style="list-style-type: none"> • Articles 8-10, 16, 36, and 37 of the Federal Law on Protection of Personal Data held by Private Parties. Regulating when consent from the data owner is needed, the type of consent needed and the exemption cases. Furthermore, articles 36 and 37 state the consent clauses needed for transferences and the transferences without consent permitted under certain scenarios. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Articles 11-16, 17, 18-22, 40 – 43 and Chapter IV (articles 67 – 76) of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the characteristics of consent and the obligations

		<p>to comply with the principles of consent and purpose, e.g., the data controller must obtain consent to process unless it is exempted in article 10 of the Law or article 17 of the Regulations. The consent must be referred to a determined purpose or purposes settle in the Privacy Notice. When personal data is collected directly from the data owner, consent should be obtained before any phase of treatment. They also describe the characteristics of the tacit and expressed consent, their modalities and exceptions, as well as, the obligations of data controllers and the rights of data owners in order to revoke consent. Moreover articles 40 – 43 explain how to comply with the Principle of Purpose, how to differentiate between purposes, how to oppose a determined purpose and when are different purposes allowed. Additionally, the Regulation states in Chapter IV the reach, conditions, and obligations to transfer personal data, for domestic and international transferences.</p>
--	--	---

INTEGRITY OF PERSONAL INFORMATION

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

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
<p>21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.</p>	<p>Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use.</p> <p><u>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.</u></p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Article 11 of the Federal Law on Protection of Personal Data held by Private Parties, which states that the data controller shall ensure that the personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected, this obligation corresponds to the Quality principle which also obliges the data controller to cancel the data as soon as its purposes stated in the Privacy Notice have been fulfilled. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Articles 36 - 39 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the Principle of Quality by stating that quality is preserved when the personal data being processed is exact, complete, appropriate, correct and updated, depending on the purpose it is used for. Furthermore, they set forth the retention periods and the procedures to keep, block and delete

		personal data.
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	<p>Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information <u>such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method.</u> <u>The Accountability Agent must verify that this process is in place and operational.</u></p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Article 11 of the Federal Law on Protection of Personal Data held by Private Parties, which states that the data controller shall ensure that the personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected, this obligation corresponds to the Quality principle which also obliges the data controller to cancel the data as soon as its purposes stated in the Privacy Notice have been fulfill. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Articles 36 - 39 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the Principle of Quality by stating that quality is preserved when the personal data being processed is exact, complete, appropriate, correct and updated, depending on the purpose it is used for. Furthermore, they set forth the retention periods and the procedures to keep, block and delete personal data.
23. Where inaccurate, incomplete or out of date information will affect the	Where the Applicant answers YES , the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate	<ul style="list-style-type: none"> • Article 11 of the Federal Law on Protection of Personal Data held by Private Parties, which states that the data controller shall ensure that the

<p>purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.</p>	<p>corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant’s behalf.</p> <p>The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant’s behalf.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.</p>	<p>personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected, this obligation corresponds to the Quality principle which also obliges the data controller to cancel the data as soon as its purposes stated in the Privacy Notice have been fulfill.</p> <ul style="list-style-type: none"> • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Articles 36 - 39 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the Principle of Quality by stating that quality is preserved when the personal data being processed is exact, complete, appropriate, correct and updated, depending on the purpose it is used for. Furthermore, they set forth the retention periods and the procedures to keep, block and delete personal data.
<p>24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the</p>	<p>Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed.</p> <p>The Accountability Agent must verify that these procedures are in place and operational.</p> <p>Where the Applicant answers NO, the Accountability</p>	<ul style="list-style-type: none"> • Article 11 of the Federal Law on Protection of Personal Data held by Private Parties, which states that the data controller shall ensure that the personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected, this obligation corresponds to the Quality principle which also obliges the data controller to cancel the data as soon as its purposes stated in the Privacy Notice have been

<p>corrections to other third parties to whom the personal information was disclosed? If YES, describe.</p>	<p>Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.</p>	<p>fulfill.</p> <ul style="list-style-type: none"> • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Articles 36 - 39 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the Principle of Quality by stating that quality is preserved when the personal data being processed is exact, complete, appropriate, correct and updated, depending on the purpose it is used for. Furthermore, they set forth the retention periods and the procedures to keep, block and delete personal data.
<p>25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?</p>	<p>Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated.</p> <p>The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service</p>	<ul style="list-style-type: none"> • Article 11 of the Federal Law on Protection of Personal Data held by Private Parties, which states that the data controller shall ensure that the personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected, this obligation corresponds to the Quality principle which also obliges the data controller to cancel the data as soon as its purposes stated in the Privacy Notice have been fulfill. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal

	<p>providers.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.</p>	<p>Data.</p> <ul style="list-style-type: none">• Articles 36 - 39 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties complement the Principle of Quality by stating that quality is preserved when the personal data being processed is exact, complete, appropriate, correct and updated, depending on the purpose it is used for. Furthermore, they set forth the retention periods and the procedures to keep, block and delete personal data.
--	--	---

SECURITY SAFEGUARDS

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

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
26. Have you implemented an information security policy?	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of this written policy.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Articles 19, 20 and 21 of the Federal Law on Protection of Personal Data held by Private Parties set forth the duties for data controllers in terms of security, security breaches and confidentiality. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Article 4, fraction IV and article 50, fraction III of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the mandatory nature of the Regulations regarding personal data security and when data controllers and data processors have to implement security measures. Articles 57-66 explain how to determine security measures, actions that must be enacted, actualizations, among others. For example they determine the elements to take into account to implement security measures, as well as, the actions the data controller must implement in order to maintain data security

		<p>through time and the minimal actions that are established in case a data breach occurs.</p>
<p>27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?</p>	<p>Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include:</p> <ul style="list-style-type: none"> • <u>Authentication and access control (eg password protections)</u> • <u>Encryption</u> • <u>Boundary protection (eg firewalls, intrusion detection)</u> • <u>Audit logging</u> • <u>Monitoring (eg external and internal audits, vulnerability scans)</u> • <u>Other (specify)</u> <p>The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.</p> <p>Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held.</p> <p>The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is</p>	<ul style="list-style-type: none"> • Articles 19, 20 and 21 of the Federal Law on Protection of Personal Data held by Private Parties set forth the duties for data controllers in terms of security, security breaches and confidentiality. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Article 4, fraction IV and article 50, fraction III of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the mandatory nature of the Regulations regarding personal data security and when data controllers and data processors have to implement security measures. Articles 57-66 explain how to determine security measures, actions that must be enacted, actualizations, among others. For example they determine the elements to take into account to implement security measures, as well as, the actions the data controller must implement in order to maintain data security through time and the minimal actions that are established in case a data breach occurs.

	<p>transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.</p> <p>Where the Applicant indicates that it has NO physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.</p>	
<p>28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.</p>	<p>Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified.</p> <p>The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.</p>	<ul style="list-style-type: none"> • Articles 19, 20 and 21 of the Federal Law on Protection of Personal Data held by Private Parties set forth the duties for data controllers in terms of security, security breaches and confidentiality. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Article 4, fraction IV and article 50, fraction III of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the mandatory nature of the Regulations regarding personal data security and when data controllers and data processors have to implement security measures. Articles 57-66 explain how to determine security measures, actions that must be enacted, actualizations, among others. For example they determine the elements to take

		into account to implement security measures, as well as, the actions the data controller must implement in order to maintain data security through time and the minimal actions that are established in case a data breach occurs.
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	<p>The Accountability Agent must verify that the Applicant's employees are aware of the importance of, <u>and obligations respecting</u>, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include:</p> <ul style="list-style-type: none"> • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) <p>Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Articles 19, 20 and 21 of the Federal Law on Protection of Personal Data held by Private Parties set forth the duties for data controllers in terms of security, security breaches and confidentiality. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Article 4, fraction IV and article 50, fraction III of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the mandatory nature of the Regulations regarding personal data security and when data controllers and data processors have to implement security measures. Articles 57-66 explain how to determine security measures, actions that must be enacted, actualizations, among others. For example they determine the elements to take into account to implement security measures, as well as, the actions the data controller must implement in order to maintain data security through time and the minimal actions that are established in case a data breach occurs.
30. Have you implemented	Where the Applicant answers YES (to questions 30.a to	<ul style="list-style-type: none"> • Articles 19, 20 and 21 of the Federal Law on

<p>safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through:</p> <p>30.a) Employee training and management or other safeguards?</p> <p>30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?</p> <p>30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?</p> <p>30.d) Physical security?</p>	<p>30.d), the Accountability Agent has to verify the existence each of the safeguards.</p> <p>The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information.</p> <p>Where the Applicant answers NO (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.</p>	<p>Protection of Personal Data held by Private Parties set forth the duties for data controllers in terms of security, security breaches and confidentiality.</p> <ul style="list-style-type: none"> • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Article 4, fraction IV and article 50, fraction III of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the mandatory nature of the Regulations regarding personal data security and when data controllers and data processors have to implement security measures. Articles 57-66 explain how to determine security measures, actions that must be enacted, actualizations, among others. For example they determine the elements to take into account to implement security measures, as well as, the actions the data controller must implement in order to maintain data security through time and the minimal actions that are established in case a data breach occurs.
<p>31. Have you implemented a policy for secure disposal of personal information?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Articles 19, 20 and 21 of the Federal Law on Protection of Personal Data held by Private Parties set forth the duties for data controllers in terms of security, security breaches and confidentiality. • Articles 63-66, which describe the acts considered to be violations to the Law and the

		<p>sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data.</p> <ul style="list-style-type: none"> • Article 4, fraction IV and article 50, fraction III of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the mandatory nature of the Regulations regarding personal data security and when data controllers and data processors have to implement security measures. Articles 57-66 explain how to determine security measures, actions that must be enacted, actualizations, among others. For example they determine the elements to take into account to implement security measures, as well as, the actions the data controller must implement in order to maintain data security through time and the minimal actions that are established in case a data breach occurs.
<p>32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Articles 19, 20 and 21 of the Federal Law on Protection of Personal Data held by Private Parties set forth the duties for data controllers in terms of security, security breaches and confidentiality. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Article 4, fraction IV and article 50, fraction III of the Regulations to the Federal Law on Protection of Personal Data held by Private

		<p>Parties set forth the mandatory nature of the Regulations regarding personal data security and when data controllers and data processors have to implement security measures. Articles 57-66 explain how to determine security measures, actions that must be enacted, actualizations, among others. For example they determine the elements to take into account to implement security measures, as well as, the actions the data controller must implement in order to maintain data security through time and the minimal actions that are established in case a data breach occurs.</p>
<p>33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.</p>	<p>The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.</p>	<ul style="list-style-type: none"> • Articles 19, 20 and 21 of the Federal Law on Protection of Personal Data held by Private Parties set forth the duties for data controllers in terms of security, security breaches and confidentiality. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Article 4, fraction IV and article 50, fraction III of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the mandatory nature of the Regulations regarding personal data security and when data controllers and data processors have to implement security measures. Articles 57-66 explain how to determine security measures, actions that must be enacted, actualizations, among others. For

		<p>example they determine the elements to take into account to implement security measures, as well as, the actions the data controller must implement in order to maintain data security through time and the minimal actions that are established in case a data breach occurs.</p>
<p>34. Do you use <u>risk assessments or third-party certifications</u>? Describe below.</p>	<p>The Accountability Agent must verify that such <u>risk assessments or certifications</u> are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.</p>	<ul style="list-style-type: none"> • Articles 19, 20 and 21 of the Federal Law on Protection of Personal Data held by Private Parties set forth the duties for data controllers in terms of security, security breaches and confidentiality. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Article 4, fraction IV and article 50, fraction III of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the mandatory nature of the Regulations regarding personal data security and when data controllers and data processors have to implement security measures. Articles 57-66 explain how to determine security measures, actions that must be enacted, actualizations, among others. For example they determine the elements to take into account to implement security measures, as well as, the actions the data controller must implement in order to maintain data security through time and the minimal actions that are established in case a data breach occurs.

<p>35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by:</p> <p>35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?</p> <p>35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers?</p> <p>35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?</p>	<p>The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.</p>	<ul style="list-style-type: none"> • Articles 19, 20 and 21 of the Federal Law on Protection of Personal Data held by Private Parties set forth the duties for data controllers in terms of security, security breaches and confidentiality. • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Article 4, fraction IV and article 50, fraction III of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the mandatory nature of the Regulations regarding personal data security and when data controllers and data processors have to implement security measures. Articles 57-66 explain how to determine security measures, actions that must be enacted, actualizations, among others. For example they determine the elements to take into account to implement security measures, as well as, the actions the data controller must implement in order to maintain data security through time and the minimal actions that are established in case a data breach occurs.
---	---	--

ACCESS AND CORRECTION

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

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

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
<p>36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests.</p> <p>The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity.</p> <p>The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information.</p> <p>The personal information must be provided to individuals</p>	<ul style="list-style-type: none"> • Articles 22-35 of the Federal Law on Protection of Personal Data held by Private Parties set forth the rights of the data owners to access, rectification, cancelation and objection in order to protect their personal data. The exercise of any of these is not a prerequisite nor does it impede the exercise of another. Furthermore, within these articles are stated the procedures to exercise the rights to access, rectification, cancelation or objection, and the situations when the data controller could deny its exercise.

	<p>in an easily comprehensible way.</p> <p>The Applicant must provide the individual with a time frame indicating when the requested access will be granted.</p> <p>Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	<ul style="list-style-type: none"> • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. • Articles 2, fraction II, and 87-112 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties address the exercise of the ARCO rights, punctuating the activities data controllers will develop in order to ensure simple and, in general, cost-free procedures –except for the reproduction media costs-, specified requirements to exercise these rights and the people authorized to exercise them, as well as, the means enabled to process the Rights.
<p>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.</p> <p>37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.</p>	<p>Where the Applicant answers YES the Accountability Agent must verify each answer provided.</p> <p>The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information.</p> <p>If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate.</p> <p>Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit</p>	<ul style="list-style-type: none"> • Articles 22-35 of the Federal Law on Protection of Personal Data held by Private Parties set forth the rights of the data owners to access, rectification, cancelation and objection in order to protect their personal data. The exercise of any of these is not a prerequisite nor does it impede the exercise of another. Furthermore, within these articles are stated the procedures to exercise the rights to access, rectification, cancelation or objection, and the situations when the data controller could deny its exercise. • Articles 63-66, which describe the acts

<p>37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe.</p> <p>37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.</p> <p>37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)?</p> <p>37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.</p>	<p>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.</p>	<p>considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data.</p> <p>Articles 2, fraction II, and 87-112 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties address the exercise of the ARCO rights, punctuating the activities data controllers will develop in order to ensure simple and, in general, cost-free procedures –except for the reproduction media costs-, specified requirements to exercise these rights and the people authorized to exercise them, as well as, the means enabled to process the Rights.</p>
<p>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).</p> <p>38.a) Are your access and</p>	<p>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.</p> <p>If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate.</p> <p>All access and correction mechanisms have to be simple</p>	<ul style="list-style-type: none"> • Articles 22-35 of the Federal Law on Protection of Personal Data held by Private Parties set forth the rights of the data owners to access, rectification, cancelation and objection in order to protect their personal data. The exercise of any of these is not a prerequisite nor does it impede the exercise of another. Furthermore, within these articles are stated the procedures to exercise the rights to access, rectification, cancelation or

<p>correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.</p> <p>38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion?</p> <p>38.c) Do you make such corrections or deletions within a reasonable time frame following an individual’s request for correction or deletion?</p> <p>38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted?</p> <p>38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the</p>	<p>and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual.</p> <p>Where the Applicant answers NO to questions 38a-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.</p>	<p>objection, and the situations when the data controller could deny its exercise.</p> <ul style="list-style-type: none"> • Articles 63-66, which describe the acts considered to be violations to the Law and the sanctions that may be enforced by the Federal Institute for Access to Information and Personal Data. <p>Articles 2, fraction II, and 87-112 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties address the exercise of the ARCO rights, punctuating the activities data controllers will develop in order to ensure simple and, in general, cost-free procedures –except for the reproduction media costs-, specified requirements to exercise these rights and the people authorized to exercise them, as well as, the means enabled to process the Rights.</p>
---	---	---

denial of access or correction?		
---------------------------------	--	--

ACCOUNTABILITY

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

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
<p>39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe.</p> <ul style="list-style-type: none"> • Internal guidelines or policies (if applicable, describe how implemented) _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____ • Compliance with self-regulatory applicant code _____ 	<p>The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller. • Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data

<p>and/or rules ____</p> <ul style="list-style-type: none"> • Other (describe) ____ 		<p>processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner.</p> <ul style="list-style-type: none"> • Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law. • Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner's interests and the reasonable expectation of privacy. 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. • Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the
--	--	--

		<p>relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.</p>
<p>40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant’s overall compliance with these Principles.</p> <p>The Applicant must designate an individual or individuals to be responsible for the Applicant’s overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller. • Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner. • Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law.

		<ul style="list-style-type: none"> • Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner’s interests and the reasonable expectation of privacy. 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. • Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.
<p>41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as:</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of

	<ol style="list-style-type: none"> 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.</p>	<p>legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller.</p> <ul style="list-style-type: none"> • Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner. • Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law. • Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner's interests and the reasonable expectation of privacy. The data controller has the obligation to safeguard and respond for the
--	---	---

		<p>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.</p> <ul style="list-style-type: none"> • Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.
<p>42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller.

		<ul style="list-style-type: none">• Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner.• Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law.• Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner's interests and the reasonable expectation of privacy. 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.• Articles 50-55 and Chapter IV Personal
--	--	--

		<p>Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.</p>
<p>43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.</p>	<p>The Accountability Agent must verify that the Applicant indicates what remedial action is considered.</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller. • Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner.

		<ul style="list-style-type: none"> • Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law. • Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner's interests and the reasonable expectation of privacy. 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. • Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.
44. Do you have procedures in	Where the Applicant answers YES , the Accountability	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on

<p>place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.</p>	<p>Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints.</p> <p>Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.</p>	<p>Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller.</p> <ul style="list-style-type: none"> • Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner. • Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law. • Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner's
---	---	---

		<p>interests and the reasonable expectation of privacy. 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.</p> <ul style="list-style-type: none"> • Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.
<p>45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even

		<p>when the data has been processed by a third party at the request of the data controller.</p> <ul style="list-style-type: none">• Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner.• Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law.• Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner's interests and the reasonable expectation of privacy. 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
--	--	--

		<p>or any other mechanism he deems appropriate for said purposes.</p> <ul style="list-style-type: none"> • Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.
<p>46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?</p> <ul style="list-style-type: none"> • Internal guidelines or policies _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____ • Compliance with self-regulatory applicant code _____ 	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of each type of agreement described.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller. • Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing.

<p>and/or rules _____</p> <ul style="list-style-type: none"> • Other (describe) _____ 		<p>Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner.</p> <ul style="list-style-type: none"> • Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law. • Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner's interests and the reasonable expectation of privacy. 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. • Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data
--	--	---

		processors and third parties assume in domestic and international transfers.
<p>47. Do these agreements generally require that personal information processors, agents, contractors or other service providers:</p> <ul style="list-style-type: none"> • Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement? _____ • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____ • Follow instructions provided by you relating to the manner in which your personal information must be handled? _____ • Impose restrictions on subcontracting unless with your consent? _____ • Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____ 	<p>The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller. • Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner. • Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law. • Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties

<ul style="list-style-type: none"> • Notify the Applicant in the case of a breach of the personal information of the Applicant’s customers? • Other (describe) _____ 		<p>set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner’s interests and the reasonable expectation of privacy. 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.</p> <ul style="list-style-type: none"> • Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.
<p>48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your</p>	<p>The Accountability Agent must verify the existence of such self-assessments.</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle,

<p>instructions and/or agreements/contracts? If YES, describe below.</p>		<p>and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller.</p> <ul style="list-style-type: none"> • Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner. • Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law. • Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner's interests and the reasonable expectation of privacy. 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
--	--	--

		<p>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.</p> <ul style="list-style-type: none"> • Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.
<p>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.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of the Applicant’s procedures such as spot checking or monitoring mechanisms.</p> <p>Where the Applicant answers NO, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller. • Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or

		<p>foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner.</p> <ul style="list-style-type: none">• Articles 63-66 detail the violations in which the data controller might incur and which will be sanctioned by the Law.• Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner's interests and the reasonable expectation of privacy. 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.• Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed
--	--	--

		<p>by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.</p>
<p>50. Do you disclose personal information to other recipient <u>persons or organizations</u> 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?</p>	<p>If YES, the Accountability Agent must ask the Applicant to explain:</p> <p>(1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and</p> <p>(2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.</p>	<ul style="list-style-type: none"> • Articles 6 and 14 of the Federal Law on Protection of Personal Data held by Private Parties specify that data controllers shall adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality under the Law to comply with the accountability principle, and that the data controller shall ensure compliance with these principles and adopt all necessary measures for their application, which will be applicable even when the data has been processed by a third party at the request of the data controller. • Article 36 and 37 these articles set forth that where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, he must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Specifying the cases in which domestic or international data transfers may be carried out without the consent of the data owner. • Articles 63-66 detail the violations in which the data controller might incur and

		<p>which will be sanctioned by the Law.</p> <ul style="list-style-type: none"> • Articles 47 and 48 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties set forth the principle of Accountability and the measures that may be adopted by the data controller to guarantee due processing, favoring the data owner’s interests and the reasonable expectation of privacy. 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. • Articles 50-55 and Chapter IV Personal Data Transfer articles 67 – 76 specify the obligations of the data processor as regards the processing he carries out as instructed by the data controller, as well as, the relationship between data controller and data processor. Chapter IV specifies the responsibilities that data controllers, data processors and third parties assume in domestic and international transfers.
--	--	--