

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Information Privacy Individual Action Plan**

Mexico (2012)

|  | APEC Principle /Commentary | **Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [[1]](#footnote-1)** | **Provision[[2]](#footnote-2)** | **Sanction[[3]](#footnote-3)** | **Results/ Status[[4]](#footnote-4)** |
| --- | --- | --- | --- | --- | --- |
| A | Is privacy a constitutionally protected right in your economy? | Yes, in 2009 two amendments to constitutional articles 16 and 73 were published with the purpose of setting the *recognition to the right of personal data protection as fundamental and autonomous* (article 16) and to *provide the Federal Congress with the power to rule in matters related to data held by private parties and its protections* (article 73).  In this matter, the **Federal Law on Protection of Personal Data held by Private Parties** was published in the Federal Official Gazette on June 5th, 2010. |  |  |  |
| B | If not, what other available legislation deals with privacy or confidentiality of personal information. | 1. Federal Consumer Protection Law (*Ley Federal De Protección Al Consumidor*). 2. Regulations to the Federal Law on Protection of Personal Data held by Private Parties (*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*). The Regulations where published in the Federal Official Gazette on December 21st, 2011 3. Federal Public Government Information transparency and Access law (*Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*). 4. Federal Tax Code (*Código Fiscal De La Federación*) 5. Federal Code of Electoral Institutions and Procedures (*Código Federal de Instituciones y Procedimientos Electorales*) 6. Federal Public Administration Services Law (*Ley Federal del Servicio Profesional de Carrera*) 7. Copyright Act[[5]](#footnote-5) (*Ley Federal del Derecho de Autor*)[[6]](#footnote-6) 8. Credit Information Company Act (*Ley para Regular las Sociedades de Información Crediticia*)    * Mexican Trustmark |  |  |  |
| 1 | ***I Preventing Harm***  **(Ref. Para. 14)**  Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information. | Federal Law on Protection of Personal Data held by Private Parties.  Regulations to the Federal Law on Protection of Personal Data held by Private Parties | Article 6. Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law.  Article 7. Personal data must be collected and processed in a lawful manner in accordance with the provisions established by this Law and other applicable regulations.  Personal data must not be obtained through deceptive or fraudulent means.  In all processing of personal data, it is presumed that there is a reasonable expectation of privacy, understood as the trust any one person places in another for personal data provided to be treated pursuant to any agreement of the parties in the terms established by this Law.  Article 8. All processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law.  Consent will be express when such is communicated verbally, in writing, by electronic or optical means or via any other technology, or by unmistakable indications.  It will be understood that the data owner tacitly consents to the processing of his data when, once the privacy notice has been made available to him, he does not express objection.  Financial or asset data will require the express consent of the data owner, except as provided in Articles 10 and 37 of this Law.  Consent may be revoked at any time without retroactive effects being attributed thereto. For revocation of consent, the data controller must, in the privacy notice, establish the mechanisms and procedures for such action.  Article 11. The data controller shall ensure that personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected.  When the personal data is no longer necessary for the fulfillment of the objectives set forth in the privacy notice and applicable law, it must be cancelled.  The controller of the database will be required to remove information relating to nonperformance of contractual obligations, after a period of seventy-two months counted from the calendar day on which said nonperformance arose. | Article 63.- The following acts carried out by the data controller are violations of this Law:  I. Failure to satisfy the data owner's request for personal data access, rectification, cancellation or objection without well-founded reason, in the terms of this Law ;  II. Acting negligently or fraudulently in processing and responding to requests for personal data access, rectification, cancellation or objection ;  III.     III. Fraudulently declaring the inexistence of personal data where such exists in whole or in part in the databases of the data controller;  IV. Processing personal data in violation of the principles established in this Law;  V. Omitting, in the privacy notice, any or all of the items referred to in Article 16 of this Law;  VI. Maintaining inaccurate personal data when such action is attributable to the data controller, or failing to perform legally due rectifications or cancellations where the data owner's rights are affected;  VII. Failure to comply with the notice referred to in section I of Article 64;  VIII. Breaching the duty of confidentiality established in Article 21 of this Law;  IX. Materially changing the original data processing purpose, without observing the provisions of Article 12;  X. Transferring data to third parties without providing them with the privacy notice containing the limitations to which the data owner has conditioned data disclosure;  XI. Compromising the security of databases, sites, programs or equipment, where attributable to the data controller;  XII. Carrying out the transfer or assignment of personal data outside of the cases where it is permitted under this Law;  XIII. Collecting or transferring personal data without the express consent of the data owner, in the cases where this is required;  XIV. Obstructing verification actions of the authority;  XV. Collecting data in a deceptive and fraudulent manner;  XVI. Continuing with the illegitimate use of personal data when the Institute or the data owners have requested such use be ended;  XVII. Processing personal data in a way that affects or impedes the exercise of the rights of access, rectification, cancellation and objection set forth in Article 16 of the Political Constitution of the United Mexican States;  XVIII. Creating databases in violation of the provisions of Article 9, second paragraph, of this Law, and  XIX. Any breach by the data controller of the obligations pertaining thereto as established in the provisions of this Law.  Article 64.- Violations to this Law will be punished by the Institute as follows:  I. A warning instructing the data controller to carry out the actions requested by the data owner, under the terms established by this Law, in the cases described in section I of the preceding article;  II. A fine from 100 to 160,000 days of the Mexico City minimum wage, in the cases described in sections II to VII of the preceding article;  III. A fine from 200 to 320,000 days of the Mexico City minimum wage, in the cases described in sections VIII to XVIII of the preceding article; and  IV. In the event of repeated occurrences of the violations described in the preceding paragraphs, an additional fine will be imposed from 100 to 320,000 days of the current Mexico City minimum wage. With regard to violations committed in processing sensitive data, sanctions may be increased up to double the established amounts.  IV. |  |
| 2 | ***II Notice***  **(Ref. Para. 15-17)**  Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should  include:  a) the fact that personal information is being collected;  b) the purposes for which personal information is collected;  c) the types of persons or organizations to whom personal information might be disclosed;  d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;  e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.  All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.  It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information. | Federal Law on Protection of Personal Data held by Private Parties. | Article 3.- For purposes of this Law, the following definitions will apply:  Privacy Notice: Document in physical, electronic or any other format, generated by the data controller that is made available to the data owner prior to the processing of his personal data, in accordance with Article 15 of this Law.  Article 14.- The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. The data controller must take all necessary and sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship.  Article 15.- The data controller will have the obligation of providing data owners with information regarding what information is collected on them and why, through the privacy notice.  Article 16.- The privacy notice must contain at least the following information:    I. The identity and domicile of the data controller collecting the data;  II. The purposes of the data processing;  III. The options and means offered by the data controller to the data owners to limit the use or disclosure of data;  IV. The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law;  V. Where appropriate, the data transfers to be made, and  VI. The procedure and means by which the data controller will notify the data owners of changes to the privacy notice, in accordance with the provisions of this Law.  For sensitive personal data, the privacy notice must expressly state that it is dealing with this type of data. |  |  |
| 3 | ***III Collection Limitation***  **(Ref. Para. 18)**  The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned. | Federal Law on Protection of Personal Data held by Private Parties. | Article 7. Personal data must be collected and processed in a lawful manner in accordance with the provisions established by this Law and other applicable regulations.  Personal data must not be obtained through deceptive or fraudulent means.  In all processing of personal data, it is presumed that there is a reasonable expectation of privacy, understood as the trust any one person places in another for personal data provided to be treated pursuant to any agreement of the parties in the terms established by this Law.  Article 8. All processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law.  Article 12. Processing of personal data must be limited to the fulfillment of the purposes set out in the privacy notice. If the data controller intends to process data for another purpose which is not compatible or analogous to the purposes set out in the privacy notice, the data owner's consent must be obtained again. |  |  |
| 4 | ***IV Use of Personal Information***  **(Ref. Para. 19)**  Personal information collected should be used only to fulfill the purposes of  collection and other compatible or related purposes except:  a) with the consent of the individual whose personal information is collected;  b) when necessary to provide a service or product requested by the individual; or,  c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect. | Federal Law on Protection of Personal Data held by Private Parties. | Article 13. Processing of personal data will be done as necessary, appropriate and relevant with relation to the purposes set out in the privacy notice. In particular, for sensitive personal data, the data controller must make reasonable efforts to limit the processing period thereof to the minimum required.  Article 10. Consent for processing of personal data will not be necessary where:  I. Any Law so provides;  II. The data is contained in publicly available sources;  III. The personal data is subject to a prior dissociation procedure;  IV. It has the purpose of fulfilling obligations under a legal relationship between the data owner and the data controller;  V. There is an emergency situation that could potentially harm an individual in his person or property;  VI. It is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data owner is unable to give consent in the terms established by the General Health Law and other applicable laws, and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or  VII. A resolution is issued by a competent authority. |  |  |
| 5 | ***V Choice***  **(Ref. Para. 20)**  Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be  appropriate for personal information controllers to provide these mechanisms when collecting publicly available information. | Federal Law on Protection of Personal Data held by Private Parties. | Article 6. Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law.  Article 8. All processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law.  Consent will be express when such is communicated verbally, in writing, by electronic or optical means or via any other technology, or by unmistakable indications.  It will be understood that the data owner tacitly consents to the processing of his data when, once the privacy notice has been made available to him, he does not express objection.  Financial or asset data will require the express consent of the data owner, except as provided in Articles 10 and 37 of this Law.  Consent may be revoked at any time without retroactive effects being attributed thereto. For revocation of consent, the data controller must, in the privacy notice, establish the mechanisms and procedures for such action.  Article 9. In the case of sensitive personal data, the data controller must obtain express written consent from the data owner for processing, through said data owner's signature, electronic signature, or any authentication mechanism established for such a purpose.  Databases containing sensitive personal data may not be created without justification of their creation for purposes that are legitimate, concrete and consistent with the explicit objectives or activities pursued by the regulated party.  Article 10. Consent for processing of personal data will not be necessary where:  I. Any Law so provides;  II. The data is contained in publicly available sources;  III. The personal data is subject to a prior dissociation procedure;  IV. It has the purpose of fulfilling obligations under a legal relationship between the data owner and the data controller;  V. There is an emergency situation that could potentially harm an individual in his person or property;  VI. It is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data owner is unable to give consent in the terms established by the General Health Law and other applicable laws, and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or  VII. A resolution is issued by a competent authority.  Article 12. Processing of personal data must be limited to fulfillment of the purposes set out in the privacy notice. If the data controller intends to process data for another purpose which is not compatible or analogous to the purposes set out in the privacy notice, the data owner's consent must be obtained again. | **CHAPTER XI**  **Crimes Relating to Unlawful Processing of Personal Data**  Article 67. Three months to three years imprisonment will be imposed on any person who, authorized to process personal data, for profit, causes a security breach affecting the databases under his custody.  Article 68. Six months to five years imprisonment will be imposed on any person who, with the aim of achieving unlawful profit, processes personal data deceitfully, taking advantage of an error of the data owner or the person authorized to transmit such data.  Article 69. With regard to sensitive personal data, the penalties referred to in this chapter will be doubled. |  |
| 6 | ***VI Integrity of Personal Information***  **(Ref. Para. 21)**  Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use. | Federal Law on Protection of Personal Data held by Private Parties. | Article 11. The data controller shall ensure that personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected.  When the personal data is no longer necessary for the fulfillment of the objectives set forth in the privacy notice and applicable law, it must be cancelled.  The controller of the database will be required to remove information relating to nonperformance of contractual obligations, after a period of seventy-two months counted from the calendar day on which said nonperformance arose. |  |  |
| 7 | ***VII Security Safeguards***  **(Ref. Para. 22)**  Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. | Federal Law on Protection of Personal Data held by Private Parties. | Article 19. All responsible parties that process personal data must establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing.  Data controllers will not adopt security measures inferior to those they keep to manage their own information. Moreover, risk involved, potential consequences for the data owners, sensitivity of the data, and technological development will be taken into account.  Article 20. Security breaches occurring at any stage of processing that materially affect the property or moral rights of data owners will be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights. | Article 39. The Institute has the following responsibilities:  VI. Hear and issue decisions in rights protection and verification procedures as set forth in this Law, and impose penalties as appropriate  Article 62. The penalty application procedure will begin with notice sent by the Institute to the alleged offender with regard to the facts that originated the procedure and will grant a period of fifteen days to present evidence and state formal arguments in writing. Where no evidence is presented, the Institute will arrive at a decision through the evidence at its disposal.  12 (First Section) OFFICIAL GAZETTE Monday, July 5, 2010  The Institute will admit evidence it deems relevant and introduce it. In addition, it may request any other evidence it deems necessary from the alleged offender. After introduction of evidence, the Institute will notify the alleged offender of its right to, if it so considers necessary, present its arguments within five days of notification.  The Institute, after analyzing the evidence and other elements of proof it deems relevant, will issue a final decision within fifty days after the date on which it initiated the penalty procedure. Notice of this decision must be given to the parties.  Where there is good cause, the Plenum of the Institute may extend this deadline a single time for a period of equal length.  The Regulations will describe the form, terms and periods for the penalty application procedure, including presentation of evidence and arguments, hearings and end of proceedings.  Article 66. The penalties specified in this chapter will be imposed without prejudice to any applicable civil or criminal liability. |  |
| 8 | ***VIII Access and Correction***  **(Ref. Para. 23-25)**  Individuals should be able to:  a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;  b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;  i. within a reasonable time;  ii. at a charge, if any, that is not excessive;  iii. in a reasonable manner;  iv. in a form that is generally understandable; and,  c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.  Such access and opportunity for correction should be provided except where:  (i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual’s privacy in the case in question;  (ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or  (iii) the information privacy of persons other than the individual would be violated.  If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial. | Federal Law on Protection of Personal Data held by Private Parties. | Article 22. Any data owner, or, where appropriate, his legal representative, may exercise the rights of access, rectification, cancellation and objection under this Law. The exercise of any of these is not a prerequisite nor does it impede the exercise of another. Personal data must be preserved in such a way as to allow the exercise of these rights without delay.  Article 23. Data owners will have the right to access their personal data held by the data controller as well as to be informed of the privacy notice to which processing is subject.  Article 24. The data owner will have the right to rectify data if it is inaccurate or incomplete.  0Article 28. The data owner or his legal representative may at any time make a request to the data controller for access, rectification, cancellation or objection in relation to the personal data concerning him.  Article 29. The access, rectification, cancellation or objection request must include the following:  I. The data owner's name and address or other means to notify him of the response to his request;  II. Documents establishing the identity or, where appropriate, legal representation of the data owner;  III. A clear and precise description of the personal data with regard to which the data owner seeks to exercise any of the abovementioned rights.  IV. Any other item or document that facilitates locating the personal data.  Article 30. All data controllers must designate a personal data person or department who will process requests from data owners for the exercise of the rights referred to in this Law. In addition, data controllers will promote protection of personal data within their organizations.  Article 31. In the case of requests for rectification of personal data, the data owner must indicate, in addition to that which is specified in the preceding article of this Law, the changes to be made, and provide documentation supporting the request.  Article 32. The data controller will notify the data owner, within a maximum of twenty days counted from the date of receipt of the request for access, rectification, cancellation or objection, of the determination made, so that, where appropriate, same will become effective within fifteen days from the date on which the notice is provided. For personal data access requests, delivery will be made upon proof of identity of the requesting party or legal representative.  The aforementioned time periods may be extended a single time by a period of equal length, provided that such action is justified by the circumstances of the case.  Article 33. The obligation to provide access to information will be fulfilled when the personal data is made available to the data owner; or, by issuing uncertified copies, electronic documents or any other means established by the data controller in the privacy notice.  In the event that the data owner requests access to data from a person or entity who he presumes is the data controller and said person or entity proves not to be such, it will be sufficient for said person or entity to so indicate to the data owner by any of the means referred to in the preceding paragraph, for the request to be considered properly fulfilled.  Article 34. The data controller may deny access to personal data or refuse the rectification, cancellation or objection with relation thereto in the following cases:  I. Where the requesting party is not the subject of the personal data, or the legal representative is not duly accredited for such purposes;  II. Where the requesting party's personal data is not found in the data controller's database;  III. Where the rights of a third party are adversely affected;  IV. Where there is any legal impediment, or decision of a competent authority, restricting access to the personal data or not allowing the rectification, cancellation or objection with relation thereto, and  V. Where the rectification, cancellation or objection has been previously performed.  The refusal referred to in this article may be partial, in which case the data controller will carry out the access, rectification, cancellation or objection requested by the data owner.  In all of the aforementioned cases, the data controller must notify the data owner, or, as appropriate, his legal representative, of its decision and the reason for such decision, within the periods established for such purposes, via the same means by which the request was made, attaching, where appropriate, any relevant evidence.  Article 35. The action of providing personal data will be free, and the data owner must only pay justified expenses of shipping or the cost of copying or providing data in other formats.  This right will be exercised by the data owner free of charge, upon proof of his identity to the data controller. However, if the same person repeats his request within a period of twelve months, costs will not be greater than three days of the General Current Minimum Wage in Mexico City, unless there are material changes to the privacy notice that prompt new queries.  The data owner may file a data protection request due to the response received or lack of response from the data controller, in accordance with the provisions of the following Chapter.  esté |  |  |
| 9 | ***IX Accountability***  **(Ref. Para. 26)**  A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles. | Federal Law on Protection of Personal Data held by Private Parties.  Regulations to the Federal Law on Protection of Personal Data held by Private Parties. | Article 6. Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law  Article 14.- The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. The data controller must take all necessary and sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship.  Article 47.-The data controller shall make reasonable efforts to limit the processing of personal data to the minimum necessary, in accordance with the processing carried out  Article 48.-Pursuant to Articles 6 and 14 of the Law, the data controller has the obligation to safeguard and respond for the processing of the personal data he guards or collects, or for those he communicated to a data processor whether the latter is in Mexican territory or not.  To comply with this obligation, the data controller may use standards, international best practices, corporate policies, self-regulation schemes or any other mechanism he deems appropriate for said purposes.  Article 49.- Pursuant to Article 14 of the Law, the data collector shall adopt measures to guarantee the due processing, favoring the data owner’s interests and the reasonable expectation of privacy.  The measures that may be adopted by the data controller include, indicatively but without limitation thereto, the following:   1. Prepare mandatory and enforceable privacy policies and programs within the data controller’s organization; 2. Implement a training, updating and awareness program for the personnel as regards the obligations in matters of protection of personal data; ; 3. Establish an internal supervision and oversight system and/or external audits to verify the compliance with privacy policies; 4. Allocate resources to implement privacy programs and policies; 5. Implement a procedure to address the risk for the protection of personal data due to the implementation of new products, services, technologies and business models, as well as mitigate them; 6. Periodically review the security policies and programs to determine the modifications required; 7. Establish procedures to receive and answer questions and complaints of the data owners in connection with their personal data; 8. Have mechanisms to comply with the privacy policies and programs, as well as sanctions for the breach thereof; 9. Establish measures to secure personal data, that is, a set of technical and administrative actions to guarantee the compliance with the principles and obligations stated in the Law and the Regulations hereof, and/or 10. Establish measures for the traceability of personal data, that is, actions, measures and technical procedures to trace personal data during their processing.   Article 50.- The data processor shall have the following obligations as regards the processing he carries out as instructed by the data controller:   1. Only process personal data according to the data controller’s instructions; 2. Refrain from processing personal data for purposes different from those informed by the data collector; 3. Implement security measures in accordance with the Law, the Regulations and other applicable provisions; 4. Maintain confidentiality as regards processed personal data; 5. Delete the personal data processed once the legal relationship with the data controller is terminated and/or as informed by the data controller, provided there is no legal provision requiring the retention of personal data, and 6. Refrain from transferring personal data except when the data controller so determines it, when the communication derives from an outsourcing or when the competent authority so requires it.   The agreements between the data controller and the data processor related to the processing shall be in accordance with the corresponding privacy notice.  Article 51.-The relationship between the data controller and the data processor shall be established by an agreement or other legal instrument determined by the data controller to prove its existence, scope and content.  ar. |  |  |
| C | Network point of contact arrangements[[7]](#footnote-7) |  | Contact details will be made available to APEC members through the APEC Secretariat. |  |  |

-- // --

1. *Note here the legislation, rule, code, framework or other privacy protection scheme. Where possible please provide the URL for the website where the legislation or arrangement is available.* [↑](#footnote-ref-1)
2. *Insert the full text or summary of the provisions of your privacy protection scheme(s) that correspond to the APEC Privacy Principles identified in the column titled “APEC Principle/ Commentary”.* [↑](#footnote-ref-2)
3. *Sanctions should include the nature of the remedies available, the means by which they are obtained, and by whom (for example, government, local law enforcement, private right of action, etc.).*  [↑](#footnote-ref-3)
4. *Identify areas where the practice and the intent of the principle need further consideration; and identify the status of the economies’ practice, for example enacted, introduced, draft.  If your legislation, rule, code, framework or other privacy protection scheme is at the drafting or proposal stage and has not yet been enacted or implemented, please indicate here and provide any other useful comments."* [↑](#footnote-ref-4)
5. *Not necessarily copyrights* [↑](#footnote-ref-5)
6. *About the protection of Data bases* [↑](#footnote-ref-6)
7. *Please provide contact details such as name and/or title, address, telephone and email contacts. This information will not be published but will be made available to economies.* [↑](#footnote-ref-7)