COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 16 October 2017 T-PD(2017)17

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

OPINION ON THE REQUEST FOR ACCESSION BY THE UNITED MEXICAN STATES

Directorate General of Human Rights and Rule of Law

Introduction

On 28 August 2017, the Secretary General of the Council of Europe received a letter dated 25 August 2017 informing him that the United Mexican States wished to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter, "Convention 108" or "the Convention") and to its Additional Protocol regarding supervisory authorities and transborder data flows (hereinafter "Additional Protocol").

The Consultative Committee of Convention 108 would point out that, in 2008, it referred to the Committee of Ministers its recommendation for non-member states with data protection legislation in compliance with Convention 108 to be invited to accede to the Convention. The Ministers' Deputies took note of this recommendation and agreed to examine every accession request in the light of it (1031st meeting, 2 July 2008).

Opinion

In accordance with Article 4 of Convention 108, each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in the Convention (Chapter II). Pursuant to Article 3.1 of the Additional Protocol, the Parties shall regard the provisions of Articles 1 and 2 of the Protocol as additional articles to the Convention and all the provisions of the Convention shall apply accordingly.

Having taken note of the Constitution of the United Mexican States (Articles 1, 16§2, 6A Fraction II, III, VIII, 73, 116 and 133) which respectively guarantee the enjoyment of human rights, the rights to private life and to the protection of one's personal data, data subjects' rights (access, correction, erasure, objection), the institution of an autonomous and independent body in charge of ensuring compliance with the right to personal data protection ("the National Institute of Transparency, Access to Information and Protection of Personal data ", hereinafter "INAI"), its composition, the powers of the Congress of the Union of Mexican States to legislate on this issue and the rank of international treaties in the domestic legal order.

Having examined[1] the Federal Law of 2010 on the Protection of Personal Data held by Private Parties (hereinafter "the Federal Law"), the Regulations to the Federal Law on the Protection of personal Data held by Private Parties of 2010 (hereinafter "the Regulations") and the General Law on the Protection of Personal Data held by Obligated Parties of 2017 (hereinafter "the General Law"), the Committee notes the following:

1. Object and purpose (Article 1 of Convention 108)

The purpose of the Federal Law is set out in its Article 1, namely *"protecting personal data held by private parties, in order to regulate its legitimate, controlled and informed processing, to ensure the privacy and the right to informational self-determination of individuals*".

[1] Legal texts provided with the request:

- https://mycloud.coe.int/index.php/s/MRj0JVXMXeyxTGy
- https://mycloud.coe.int/index.php/s/9360xnCcX5jAMrw

On the basis of an English translation of the laws and regulations.
Original versions are available at:
The Federal Law: http://inicio.ifai.org.mx/LFPDPPP/LFPDPPP.pdf
The Regulations: http://inicio.ifai.org.mx/PROTECCIONDEDATOSPERSONALES/RLFPDPP.pdf
The General Law: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

The purpose of the General Law is laid down in its Article 1, stating that this law "*is the regulatory law of articles 6, Base A and 16, second paragraph of the Political Constitution of the United Mexican States, regarding the protection of personal data held by obligated parties*" and "*its purpose is that of establishing the bases, principles and procedures required to uphold the right of any person to the protection of his/her personal data held by obligated parties*".

These statements comply with the purpose set forth in the provisions of Article 1 of Convention 108.

2. Definitions

The Federal Law sets out the definitions of "personal data", "data processing" and "controller" (Articles 2.a, 2.b, 2.d of Convention 108) in Articles 3(V), 3(XVIII) and 3(XIV) respectively. The Federal Law also includes a definition of the notions of "sensitive data" in Article 3(VI), "data processor' in Article 3(IX), "data owner" in Article 3(XVII) and "transfer' in Article 3(XIX). The Regulations adds a number of definitions to the ones proposed under the Federal Law and notably, the notions of "identifiable individual", "transmission" (Article 2 of the Regulations).

The General Law lays down similar definitions and also includes definitions of the notion of "assessment of impact on the protection of personal data" in Article 3(IV), consent in Article 3(VIII), filing system in Article 3(XII).

A. Personal data (Article 2.a of the Convention)

The Federal Law defines "personal data" as "*any information concerning an identified or identifiable individual*" in Article 3(V).

The General Law provides in Article 3(XXI) for a similar definition and adds to it that "*an individual is deemed to be identifiable when his/her identity may be directly or indirectly deduced from any information*"

Both laws define the data subject (referred to as 'data owner in the Federal Law) as "*the individual to whom the personal data relates*".

This definition corresponds to the one given in Article 2.a of Convention 108.

B. Automatic processing (Article 2.c of the Convention)

Article 3(XVIII) of the Federal Law defines "the processing of personal data" as "*retrieval, use, disclosure or storage of personal data by any means. Use covers any action of access, management, exploitation, transfer or disposal of personal data*".

The General Law lays down a more complete definition of data processing in Article 3(XXIV): "*Any operation or set of operations undertaken by manual or automated means applied to personal data, relating to the retrieval, use, recording, organization, preservation, preparation, utilization, communication, dissemination, storage, holding, accessing, managing, exploitation, release, transfer or disposal of personal data*".

Article 2.c of Convention 108 contains supplementary operations in the open-ended list, which also refers to the "carrying out of logical and/or arithmetical operations" on the data processed, to "alteration" and to "erasure". The Committee considers that the definition of the Federal Law may be understood as a narrower one (the General law refers to 'any operation or set of operations relating to' a particular list of actions, also appearing narrower) which would benefit from further complements, in particular with regard to the operations above-mentioned that are not listed in the definition.

C. Controller of the file (Article 2.d of the Convention)

The Federal Law defines in Article 3(XIV) the data controller as the "*individual or private legal entity that decides on the processing of personal data*." The General Law provides a similar definition in Article 3(IX), except that it applies to obligated parties.

It would be helpful to expand this definition so as to include the detail of the operations carried out which help identifying the controller under Article 2.d of Convention 108, i.e. the decision making on the purpose, the categories of personal data and the operations which should be applied to them.

D. Special categories of data (Article 6 of the Convention)

"Sensitive data" are defined in Article 3(VI) of the Federal Law as "*Personal data touching on the most private areas of the data owner's life, or whose misuse might lead to discrimination or involve a serious risk for said data owner. In particular, sensitive data is considered that which may reveal items such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views, sexual preference*." The General Law provides for a similar definition in Article 3(XXVIII).

This definition complies with Article 6 of the Convention (while personal data relating to criminal convictions are not expressly mentioned in this Article, the list given is not an exhaustive one as indicated by the term 'in particular'). Furthermore, such data are covered by a specific chapter of the General Law (Articles 80 to 82) prescribing a specific filing system with reinforced security prescriptions.

The Committee finally notes that the notion of "transfer" in the Federal Law (article 3, XIX) and in the General Law (Title V) does not only relate to transborder data flows, as is the case in Article 12 of the Convention and Article 2 of its Additional Protocol, but also to domestic operations.

3. Scope of the data protection regime (Article 3 of the Convention)

Article 1 of the Federal Law protects "personal data held by private parties" whereas Article 1 of the General Law guarantees "the protection of personal data held by obligated parties", i.e. "*any authority, entity, agency or body of the Executive, Legislative and Judiciary Branches, autonomous entities, political parties, trusts and public funds*" as well as "*Unions and any other individual or legal entity receiving and making use of public funds or acting as authority in the federal, state or local spheres*" (see Article 1, Paragraphs 5 and 6 of the General Law). The purposes of the General Law are further described in its Article 2. The data protection regime therefore applies to both the private sector (The Federal Law) and the public sector (The General Law). This scope corresponds to the scope set out in Article 3 of Convention 108.

"*Persons carrying out the collection and storage of personal data exclusively for personal use and without purposes of disclosure or commercial use*" are not subject to The Federal Law (Article 2(II) of the Federal Law) in compliance with Article 3 of the draft modernised[2] Convention 108.

The Federal Law does not specify that it shall apply "to automated or non-automated processing of personal data", and this double criteria is neither mentioned in the definition of processing (unlike for the General law which specifically refers to "*manual or automated means*" in the definition of the processing).

[2] See proposed text at: http://www.coe.int/en/web/data-protection/convention108/modernisation

Besides, Article 2 of the Federal Law specifies that "credit reporting companies under the Law Regulating Credit Reporting Companies and other applicable laws", are not regulated under the Federal Law and are subject to a *lex specialis*[3], which does not contain specific data protection provisions, implying that rights of the data subject granted under the Federal Law are not recognised in a credit reporting context, which would need to be reconsidered.

The Committee is of the opinion that the wording of the Federal Law could be reviewed to reflect the importance of covering both automated and non-automated processing in the scope of application.

The General Law applies to "*any processing of personal data contained in physical or electronic support mediums, regardless of the mode or manner in which they were created, the type of support, processing, storage and organization*" (Article 4). This appears to be compliant with Article 3 of Convention 108.

Both the Federal and the General laws refer to Public Access Sources. The Committee notes that it would be worth specifying that the data protection legislations apply to the personal data contained in these sources.

Concerning journalism, the Committee notes that the Federal Law does not refer to any derogation to the scope of application of data protection requirements.

4. Quality of data (Article 5 of the Convention)

Article 6 of the Federal Law provides that: "*Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law*." Article 7 also guarantees that the personal data is obtained and processed fairly and lawfully. Article 11 ensures that the data is relevant, correct and up-to date and not kept for longer than necessary to achieve the purpose pursued (the Committee notes that Article 11 refers to "personal data contained in databases" and recommends to suppress this limitation). The Committee underlines the requirement under Article 5 of Convention 108 that the purposes be "legitimate", which should be made clearer in the Federal Law for any processing (not solely for the processing of sensitive data). Article 13 deals with the necessity to have a limited purpose and guarantees the data are not used in a way incompatible with this purpose. Article 13 also includes the principle of data minimisation. Although the concepts used are not always called the same as in Convention 108 and it would be worth mentioning explicitly the principle of *fair* processing and adding the concept of *specific* purpose, it can be noted that, generally speaking, the guarantees laid down by the Federal Law correspond to those ensured under Article 5 of Convention 108.

The General Law which provides for the same guarantees (see Articles 16, 18, 19, 23, 25) with, in addition, a reference to the principle of "fairness" (Article 16) complies with Article 5 of Convention 108.

The Committee emphasises that with respect to the processing of data that is contained in publicly available sources (Article 10(II) of the Federal Law and Article 3(XXV) of the General Law), steps should be taken to make sure that the very nature of the data does not risk infringing the data subject's rights and fundamental freedoms.

When it comes to the legitimacy of the data processing, Article 8 of the Federal Law provides that "*all processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law*" and then describes the characteristics of consent and other legal basis for the

[3] Law to regulate credit information corporations, published in the Official Gazette on 15 January 2002, which notably contains provisions on confidentiality, security measures and rights of 'clients': http://www.banxico.org.mx/disposiciones/marco-juridico/legislacion-de-interes/leyes/%7B3D04AC1C-8A4B-2331-040C-01A03FDAD3B6%7D.pdf

processing of personal data (Article 10). The Committee welcomes this introduction and notes that the fact that consent should be “free, specific and informed” is laid down in Article 12 of the Regulations to the Federal Law (the proposed modernised Convention 108 also refers to “unambiguous” consent, thereby excluding the possibility of a tacit consent).

Article 20 of the General Law mirrors these requirements regarding consent for situations where it is the legal basis for the processing and envisages other legitimate grounds for the processing.

These provisions comply with Article 5 of Convention 108.

5. Special categories of data (Article 6 of the Convention)

Special categories of data are defined in Article 3 of the Federal Law and Article 3(XXVIII) and 21 paragraph 4 of the General Law as above-mentioned (see definitions).

Article 9 of the Federal Law provides that “*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 7 of the General Law and Article 56 of the Regulations provide for a prohibition of the processing of sensitive data, except where specific conditions are met.

However, Article 7 of the General Law also states that this prohibition does not apply in the cases set forth in Article 22 of the Law, which lists a series of cases where the data subject’s consent is not required for the processing of his/her personal data. In particular, Article 22(VIII) holds that consent is not needed “*where the personal data are contained in public access sources*.” It is important to note that public access sources might also contain sensitive data, for which automated processing might give rise to discriminatory practices or other adverse effects for the data subjects. The Committee therefore recommends to extend the prohibition of processing of sensitive data without the consent of the data subject to those data contained in public access sources.

Even if health data is categorised as sensitive data, the specific nature of the processing of health related data is not addressed either in the Federal law or in its Regulations. The General Law does not address these elements either.

The Committee encourages the insertion of specific modalities regarding the processing of health related data.

6. Data security (Article 7 of the Convention)

Article 19 of the Federal Law provides that “*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 of the Federal Law also introduces the concept of notification of security breaches to the data owner (i.e. the data subject).

It is also worth noting the provisions of Chapter III of the Regulations to the Federal Law relating to the security measures for processing personal data which implement a risk-based approach to data security (see in particular Articles 60 and 61).

The General Law mirrors the aforementioned security requirements in its Article 31, includes a risk-based approach to data security in its Article 32 and the notion of documentation of security compliance in its Articles 34, 35, 36. The General Law also provides for an obligation of the data controller to notify a security breach to the data subject and to the INAI (Article 40).

The relevant provisions applicable to the protection of personal data (the Federal law, the Regulations, the General law) comply with Article 7 of Convention 108. It can solely be regretted that the data breach notification to the supervisory authority is not foreseen under the Federal Law or under its Regulations as this would have fully anticipated the modernisation of Convention 108.

7. Additional safeguards for the data subject (Article 8 of the Convention)

Article 15 of the Federal Law provides that "*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"* and article 16 of the Federal Law details the information which should be contained in the privacy notice. The General Law provides for similar requirements (Articles 26 and 27[4]), which thus correspond to the provisions of Article 8 of Convention 108 and to the principle of transparency of the modernisation proposals.

Under Chapter III of the Federal Law and notably its Articles 22, 23, 24, 25, the rights of the data subject to access, rectification, erasure and objection are guaranteed. The Regulations to the Federal law also include a right of information of the data subject where a decision is made automatically, without human intervention (Article 112 of the Regulations). The General Law provides for similar requirements (Articles 43, 44, 45, 46 and 47). Article 57 of the General Law also provides for a right to data portability. The Federal Law and the General Law comply with Article 8 of Convention 108.

Furthermore, Article 45 of the Federal Law provides for the right of the "data owner" (i.e. data subject) to submit a claim to the INAI where his/her request to the data controller has not succeeded or is not complied with. This right complies with the requirement laid down in Article 8(d) of Convention 108.

Finally, data subjects may challenge and appeal a decision of the INAI (See Article 56 of the Federal Law and 138 and 144 of the Regulations, , Article 115 of the General law). This complies with Article 1(4) of the Additional Protocol according to which "decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts".

8. Exceptions and restrictions (Article 9 of the Convention)

The Federal Law provides for a limitation of the observance of the principles and exercise of the rights established with regard to "the protection of national security, public order, health and safety as well as the rights of third parties" (Article 4 of the Federal Law). The Committee is of the opinion that part of the interests for which the rights under the Federal Law will be restricted could be more narrowly specified and defined ("public order" being a very broad notion for instance).

Moreover, both the Federal Law and the General Law do not restrict the application of certain provisions to processing carried out by the press for the situation where they would result in a limitation of the exercise of freedom of expression.

Chapter II of the General Law, more specifically Article 80, deals with personal data collection and processing by authorities that are competent "*within the purviews of security, law enforcement and the administration of justice*" and limits the application of data protection requirements in so far as is

[4] It should be noted that the original version of the Law refers to the name of the controller and not to the name of the data subject ("*La denominación del responsable*").

"*necessary and proportional to allow them to exercise their functions regarding national security, public safety or for the prevention and prosecution of crimes*". A separate Chapter (Petition for review on matters involving national security, Articles 139 to 143) prescribes the review procedure in matters of national security.

Such provisions comply with Article 9 of Convention 108.

9. The supervisory authority (Article 1 of the Additional Protocol)

The Federal Law and the General Law seem to establish two different entities to ensure compliance with their respective requirements.

Article 38 of Chapter VI of the Federal Law provides for the establishment of a Supervisory Authority, entitled "The National Institute of Transparency, Access to Information and Protection of Personal Data (INAI)", responsible for ensuring compliance with the measures in domestic law giving effect to the principles of the Convention, in compliance with Article 1(1) of the Additional Protocol.

Article 39 of the Federal Law details its responsibilities. Article 59 mentions the powers of verifications but, not specifically "of investigation and intervention" as envisaged under Article 1(2)(a) of the Additional Protocol. However, Chapter IX of the Regulations to the Federal Law deals with "inspections" carried out by the INAI. Cooperation with other supervisory authorities is foreseen in Article 39 of the Federal law and Article 89 of the General Law.

Article 89 of the General Law lists a number of attributions of the INAI in addition to those already mentioned, such as the powers to initiate legal proceedings and to refer to judicial authorities in the context of alleged violations of personal data protection by domestic laws (Article 89(VIII)). Paragraphs (XXXII) and (XXXIII) of the same Article also enable the INAI to submit cases of unconstitutionality against "*federal or state laws and any International Treaties signed by the President of the Republic and approved by the Senate, which infringe upon the right to personal data protection*", as well as to promote "*constitutional controversies as contemplated in article 105, section I, clause I) of the Political Constitution of the United Mexican States*." The power to initiate unconstitutionality lawsuits by the INAI is also enshrined in Art. 105, Fraction II, paragraph h of the Constitution.

The composition of the INAI and the modalities of designation of its members are not addressed in the Federal Law or in the Regulations to the Federal Law. They are however addressed in a separate document submitted with the request for accession to Convention 108, entitled "4. Mexico's supervisory authority". This document recalls that the INAI has regulatory, information, verification, resolution and sanctioning powers. Besides, it refers to Article 6, Fraction VIII of the Constitution, which was made available to the Committee and which clarifies that the INAI shall carry out its tasks independently, is composed of 7 commissioners, appointed by the House of Senators after an extensive consultation of society, upon proposal of parliamentary groups, with the vote of two thirds of the members present. Commissioners shall be in office for seven years and elect their chief commissioner by secret ballot for a period of three years. Some constitutional requirements guarantee the absence of conflict of interest.

Article 116 of the Constitution also prescribes the establishment at States' level of autonomous, specialised, impartial and collegiate bodies responsible for data protection.

Activity reported of the INAI is as follows:

General Complaints filed with the INAI (2011-2016)	
Received	1361
Concluded	1294
In Process	72
Verification procedures from July 2011 to Dec. 2016	**179**
Applications received for protection of rights from Jan 2012 to Dec 2016	**728**
Of which substantiated	334
Number of requests received	**883**
Related to access requests	381
Related to Rectification requests	35
Related to Cancellation requests	310
Related to Opposition requests	157
Sanctions	
Sanctions procedures initiated	177
Sanctions procedures concluded	113
Requests regarding the public sector (obligated parties) access and correction	**296 506**
Appeals filed against the response to requests to obligated parties before the INAI	**1101**
Recommendations, models and tools developed by the INAI	
2013	7
2014	6
2015	3
2016	2
2017	3
Training in data protection delivered by the INAI	**116**
Total number of participants to these trainings	10261

Article 10 of the General Law provides for the establishment of “the National System for transparency, Access to Information and Personal Data Protection” (hereinafter “the National System”) to “contribute to maintain the right to personal data protection in full force nationwide, at the three levels of government”. The National System is regulated by the General Law on Transparency and Access to Public Information and other applicable laws and regulations which were not available for this assessment.

The General Law also refers to the INAI (Article 88 of the General Law) and to the General Law on Transparency and Access to Public Information, the Federal Law on Transparency and Access to Public information and other regulations which “may be applicable”. These legislations were not made available to the Committee. The General Law also mentions the “Guarantor bodies” (Article 91) without specifying how they differ from other existing and mentioned supervisory bodies and how their respective competences are articulated. It seems that the National Institute is the competent supervisory body at Federal level and the Guarantor bodies are competent at Federate level but this remains unclear. Consequently, the Committee notes that the provisions of the General Law relating to the National System, the INAI and to the Guarantor body should be clarified to clearly explain the allocation of competences between these different competent bodies.

Articles 146 and 147 deal with the oversight and verification powers of the Institute and the Guarantor bodies.

These provisions comply with Article 1 of the Additional Protocol.

10. Sanctions and remedies (Article 10 of the Convention)

The Federal Law provides for administrative sanctions under Article 64 in the event of a violation of the Federal law as listed in Article 63. It provides for criminal sanctions under Chapter XI and, more specifically, Articles 67 to 69. In particular, Article 64 provides for several administrative sanctions which vary from a simple warning to a fine from 100 to 320 000 of the current Mexico City minimum wage. These sanctions may be doubled when the data processing in question contains sensitive data. Articles 67 to 69 provide for criminal sanctions which vary from three months to five years of imprisonment and will be doubled if sensitive data are concerned.

The General Law also provides for administrative sanctions available to the INAI or the Guarantor bodies (Article 152) which range from public warning to monetary sanctions going from one hundred and fifty to one thousand five hundred times the daily value of the Unit of Measure and Updating (Article 153).

Individuals can file a complaint to the Supervisory Authority (Article 45 of the Federal Law) or in court. Private parties can file a petition for annulment against decisions issued by the Institute with the Federal Law and Administrative Court (Article 56). Under the General Law, "*the data subject may file a petition for review or appeal with the Institute or the Guarantor bodies, as appropriate, or else with the Transparency Unit*" (Article 94). Besides, resolutions taken by the Guarantor Body may be appealed before the INAI (Article 117).

These provisions comply with Article 10 of Convention 108.

11. Transborder flows of personal data (Article 12 of the Convention and Article 2 of its Additional Protocol)

Chapter V of the Federal Law concerns international transfers and Article 36 prescribes transfer based on the consent of the data subject, while Article 37 provides that:

"*Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases:*

I. Where the transfer is pursuant to a Law or Treaty to which Mexico is party:
II. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management;
III. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies;
IV. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party;
V. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice;
VI. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and
VII. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner."

Section III (Article 74) of the Regulations to the Federal Law relating to international transfers mentions that "*international transfers of personal data will be possible when the receiver of the* *personal data assumes the same obligations as those of the data controller transferring the personal data*". Article 76 furthermore provides for the possibility to obtain an opinion of the INAI regarding an international transfer.

The General Law also provides that "*all transfers of personal data, whether domestic or international, are subject to the data subject's consent*" (Article 65) and specifies that "*the transfer or transmittal of personal data outside the Mexican territory by the data controller can only take place when the third party recipient or data processor undertakes to protect such data in adherence to the principles and duties established in this Law and the applicable provisions on the matter*" (Article 68).

The principle of adequacy[5] or appropriateness of the level of protection is contained in Article 65 of the General Law which refers to the protection of data *"in adherence to the principles and duties established in this Law".*

Both the Federal and the General Law comply with Articles 12 of the Convention and Article 2 of its Additional Protocol.

Additional comments

The committee welcomes the introduction in the Regulations to the Federal law of the principle of accountability (Articles 47 and 48) and of a risk-based approach to the data processing carried out by the data controller (Article 48, V) thus anticipating the modernisation of Convention 108.

The Committee also welcomes the introduction of the notions of certification (Article 83 of the Regulations to the Federal Law) and of the right to data portability in the General Law.

Conclusion

In light of the above, the Consultative Committee considers that the legal framework on data protection of the United Mexican States generally complies with the principles of Convention 108 and its Additional Protocol. The Committee notes that some adjustments to the legal provisions, in line with the comments of the present opinion, would be welcome.

Based on its analysis of the applicable data protection legislation, the Consultative Committee is of the opinion that the request from the United Mexican States to be invited to accede to Convention 108 and to its additional Protocol should be given a favourable response.

[5] The principle of adequacy according to which "the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention [shall take place] only if that State or organisation ensures an adequate level of protection for the intended data transfer" and, "by way of derogation, if domestic law provides for it because of specific interests of the data subjects or legitimate prevailing interests, especially important public interests, or if safeguards which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law" is guaranteed in Article 2 of the Additional Protocol.