COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 16 June 2017 T-PD(2017)12

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

DRAFT OPINION ON THE REQUEST FOR ACCESSION BY ARGENTINA

Directorate General of Human Rights and Rule of Law

Introduction

On 29 May 2017 the Secretary General of the Council of Europe received a letter dated 15 May 2017 informing him that the Republic of Argentina wished to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter, "Convention 108").

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).

Having taken note of the Argentinian Constitution (Article 43.3) and having examined[1] the *Personal Data Protection Act* of 4 October 2000, hereinafter "the Act", the Committee notes the following.

Lastly, the Consultative Committee furthermore underlines that, following an opinion of the Article 29 Working Party,[2] the European Commission adopted a decision[3] recognising the adequacy of measures taken by Argentina in respect of protection for personal data.

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

Section 1 of the Act states that its purpose is the "*comprehensive protection of personal information recorded in files, records, databases, databanks or other technical means of data processing, either public or private for purposes of providing reports, in order to guarantee the right of individuals to their honour and privacy, as well as access to the recorded information".* The spirit of this section is the same as that of Convention 108, noting the broad interpretation given by the competent bodies (supervisory authority and courts) to the notion of "providing reports" and the fact that this criterion doesn't imply a reduction of the scope of the Act. Furthermore, Article 1 of Convention 108 which aims to secure for every individual "respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")" protects individuals with respect to the processing of any information relating to them, not only data relating to their private life.

Section 1 of the Act also refers to Article 43.3 of the Argentinian Constitution which provides that any individual may bring a "*habeas data"* action (a special judicial remedy with regard to personal data protection, whereby any individual is entitled to access data pertaining to him or her, and to request the deletion or rectification of such data if they are inaccurate or used for discriminatory purposes).

The Act has a total of 46 sections. Under Section 45 of the Act the Executive is required to adopt implementing regulations and establish appropriate supervisory bodies within 180 days of its promulgation. The provinces are encouraged to accede to the provisions of the Act. Federal jurisdiction applies in respect of data registers, files, or banks interconnected via international networks (Section 44).

2. Definitions

Section 2 of the Act lays down definitions for "personal data", "sensitive data", "data owner" (data subject) "data user" (controller), "data dissociation" ("*treatment of personal data in such a way that information obtained cannot be related to any certain or ascertainable person"*).

[1] On the basis of an unofficial English translation of the Act.
The Committee also took note of Decree No. 1558/2001 but was not able to take it into account in its analysis.
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp63_en.pdf
[3] Decision of the Commission.pdf

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

The Act defines "personal data" as *"information of any kind pertaining to certain or ascertainable physical persons or legal entities"*.

The Act furthermore defines "data owners [subjects]" as *"any physical person or legal entity having a legal domicile or local offices or branches in the country, whose data are subject to the treatment [processing] referred to in this Act".*

Although it also covers legal persons (a possibility available to Parties to the Convention) this definition corresponds to the one given in Article 2.a of Convention 108, the domicile condition only being applicable to legal persons.

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

"Sensitive data" are defined in the Act as "(*p)ersonal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, trade union membership, and information concerning health conditions or sexual habits or behaviour*."

The Committee notes that although the definition of sensitive data makes no reference to data relating to criminal convictions, such data are covered under separate provisions of the Act (Section 7.4 and, concerning data processed by the police, Section 23.3).

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

The Act mentions different data files, both public and private (Sections 22, 24, 27, 28), as well as public and private data file registers (Section 21). It defines data subject to processing and the registers in which such data are kept and defines data processing as "*(s)ystematic operations and procedures, either electronic or otherwise, that enable the collection, preservation, organisation, storage, modification, relation, evaluation, blocking, destruction, and in general, the processing of personal information, as well as its communication to third parties through reports, inquiries, interconnections or transfers*."

Although not confined to automatic processing, the definition of data processing pursuant to the Act is compatible with Article 2.c of the Convention. Indeed, it may be desirable to apply the Act even in cases where there is no automatic processing when the processing in question involves operations carried out on personal data within a structured set of data which are accessible or may be found using specific criteria or which enable the controller or anyone else to search for, combine or correlate data pertaining to a given individual.

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

The Act defines the "data user" as "(*a)ny person, either public or private, performing in its, his or her discretion the treatment of data contained in data files, registers, databases or databanks, owned by such persons or to which they may have access through a connection."* This definition corresponds to the definition given under Article 2.d of Convention 108.

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

The Act applies to the processing of personal data contained in, or for inclusion in, files, registers, bases, banks, where the data user (controller) is on Argentinian territory, and whether such processing concerns the public or private sector. This scope is apparent from the definitions of data user (controller) (Section 2) and other sections of the Act which refer to both sectors (for example Section 21 applies to "(a)ny public or private data file", and Section 35 states that action may be brought against "public or private data bank users").

Under Section 1.1 of the Act "*(i)n no case shall journalistic information sources or data bases be affected*." The Committee notes that a regime of specific exceptions would be preferable.

Lastly, although Section 28 states that the Act does not apply to opinion polls, surveys and statistics, it also provides that a data dissociation technique must be used in cases where it is impossible to ensure anonymity. The Committee notes that such data, as long as they are not made anonymous, are personal data which should thus be covered by the Act.

This scope corresponds to the scope defined in Article 3 of Convention 108. However, the Committee is of the opinion that a general provision defining the scope of the Act would add greater clarity to the text.

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

Processing of personal data cannot be carried out without the consent of the data subject or must fulfil one of the five conditions set out under Section 5.2 of the Act. These principles and bases for determining the lawfulness of personal data processing are legitimate and comply with the provisions of Article 5 of the Convention. Nonetheless, the Committee emphasises that with respect to the processing of data that are clearly in the public domain (Section 5.2a), 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 and to restrict this principle to data made public by the data subject.

Personal data collected for processing purposes must be "certain, appropriate, pertinent and not excessive with reference to the scope within and purpose for which such data were secured" (Section 4.1); data must not be collected using disloyal or fraudulent means (Section 4.2); data must not be used for any purposes other than or incompatible with the purposes for which they were collected (Section 4.3); and data must be accurate and up-to-date (Section 4.4); inaccurate or incomplete data must be deleted or replaced (Section 4.5).

These provisions of the Act comply with Article 5 of Convention 108.

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

Section 7 of the Act protects sensitive data. No one may be forced to communicate sensitive data (Section 7.1); such data may only be collected and processed in circumstances that are in the general interest and permitted by law, or for statistical or scientific purposes, and providing the data subjects cannot be identified (Section 7.2); it is forbidden to create files, banks or registers which reveal sensitive data, whether directly or indirectly (Section 7.3); data pertaining to criminal convictions may only be processed by the competent public authorities (Section 7.4). Special conditions applicable to the processing of health-related personal data are set out in Section 8 of the Act.

The relevant provisions of the Argentinian Act comply with the protection rules laid down in Article 6 of Convention 108.

6. Data security (Article 7 of the Convention)

Under Section 9 of the Act, the controller must take such technical and organisational measures as are necessary to guarantee the security and confidentiality of the personal data, in order to prevent their alteration, loss, unauthorised consultation or processing, and to allow for the detection of any intentional or unintentional distortion of such information, whether such risks stem from human conduct or the technical means used. Furthermore, Section 10 emphasises the controller's duty of professional secrecy (Section 10.1), which may only be lifted by means of legal action or on national defence, or public health and safety grounds (Section 10.2).

The relevant provisions of the Argentinian Act comply with Article 7 of Convention 108.

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

Under Section 6 of the Act, every time personal data are collected the data subject must be expressly informed in advance and in a clear manner of the purpose of the files, of their existence, of the compulsory or discretionary nature of the questions asked, of the consequences of supplying or refusing to supply the data, and of the right to access, rectify or delete the data. Furthermore, Section 13 of the Act provides "*(a)ny person may request information from the competent controlling Agency regarding the existence of data files, registers, bases or banks containing personal data, their purposes and the identity of the persons responsible therefor. The register kept for such purpose may be publicly consulted, free of charge*." Lastly, Section 15 describes the quality of the substance of information that must be provided to data subjects.

The Committee is nonetheless unsure as to the exact scope of Section 13 of the Act given that Section 41, which also concerns the right to information, no longer refers to the "controlling Agency" but only to the data

file, register or bank. Section 41 also stipulates that the reply given to the information request must state the reasons for providing or not providing the requested information.

Sections 14 and 15 establish a right of access. The right to rectify, update or delete data is established under Section 16.

Section 42 establishes the right to request the deletion, rectification and updating of data within three days of the answer given to the information request.

Section 29 provides for the creation of a supervisory authority overseeing data protection. This supervisory authority is responsible for taking all necessary steps to ensure compliance with the aims and provisions of the Act. To that end, it performs a number of different functions, including assisting and advising the data subject, in particular with regard to his or her rights as set out above.

The Committee notes that the Article 29 Working Party underlined the necessity to reinforce the independence of the supervisory authority and stands ready to assist Argentinian authorities in that respect.

These Sections of the Act comply with the provisions of Article 8 of the Convention.

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

There are no unconditional exceptions under the Argentinian Act, only limited derogations and restrictions.

Section 23.2 of the Act provides that "*processing of personal data by the armed forces, security forces, police or intelligence services for national defence or public safety purposes, without the consent of the parties concerned, shall be limited to the cases and data categories strictly necessary for fulfilment of these organisations' statutory obligations with regard to national defence, public safety or law-enforcement. In such cases, files must be specific, drawn up for that particular purpose, and categorised according to their reliability*."

Furthermore, Section 17 of the Act provides for exceptions to the right of access, rectification and deletion (Section 17.1) and the right of information (Section 17.2) in the case of public databanks. Such rights may be denied when they may affect legal or administrative proceedings in cases concerning tax or social security obligations, criminal investigations or the carrying out of environmental and health checks. Furthermore, Section 40 provides that when an exception is made under Section 17 the controller must prove that the situation falls within the scope of Section 17.

Section 40 of the Act provides that in the event of a judicial action the confidentiality obligation incumbent on controllers operating in the private sector still applies with regard to journalistic sources.

The relevant provisions of the Argentinian Act comply with Article 9 of Convention 108.

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

Data files are deemed to have been duly registered when the principles set out in the Act and in regulations deriving from the Act are respected (Section 3). Moreover, the purpose of data files must not be unlawful (Section 3). Accordingly, the Argentinian Act provides for administrative sanctions under Section 31 and criminal sanctions under Sections 32 to 43 in the event of failure to abide by the law. A breach of confidentiality or data security is a violation of personal databanks (Section 32). Section 33 defines the legal remedies available for the protection of personal data or "*habeas data*". Sections 34 to 39 set out the details regarding legal action, who is entitled to take action, the parties against whom proceedings may be brought, competent jurisdiction, the applicable procedure, and the conditions that must be met.

The provisions of the first four chapters (general provisions, general data protection principles, rights of the data subject, controllers) and Section 32 (criminal sanctions) are public order provisions (Section 44.1).

The Act complies with Article 10 of Convention 108.

10. Transborder flows of personal data (Article 12 of the Convention)

Section 12 of the Act concerns international transfers and provides that transfers of any kind of personal information to States or international organisations that fail to provide an adequate level of protection are prohibited (Section 12.1), subject to the following exceptions: international judicial cooperation, international police cooperation in the fight against organised crime or terrorism, and the exchange of medical data (Section 12.2).

Section 12 of the Act meets the requirements of Article 12 of Convention 108.

The Committee welcomes this requirement regarding adequate data protection but is unsure as to how such adequacy is ascertained. The Committee underlines that according to Article 12 of Convention 108, there can in principle be no barriers to transborder flows of personal data between Parties for the sole purpose of the protection of personal data.

Additional comments

The Committee very much welcomes Section 20 of the Act concerning objections to personal assessments, which stresses that judicial or administrative decisions must not be based solely on electronic processing of personal data. These provisions, which are in line with the modernised Convention (Article 8.a), would need to be extended so that they also cover processing by the private sector.

Moreover, whereas Sections 25 and 26 of the Act, which concern the supply of IT services and information services, go some way to defining outsourcing, an express future reference to outsourcing would be a good thing (as will be the case, for example, in the modernised Convention).

Furthermore, the Committee notes that it would also be worthwhile including a right to object in the Act, as well as a definition of data recipients.

Lastly, the Committee welcomes the fact that the Act contains a Section on direct marketing (Section 27.1).

Although the request made by Argentina only concerns accession to the Convention, the Committee would emphasise that for data protection to be effective it is important to set up a data protection authority, such as that established under Section 29 of the Act, in accordance with Article 1 of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (hereinafter "Additional Protocol"). Section 29 of the Act provides for the establishment of a supervisory body ("Controlling Agency") with authority to take all necessary steps to ensure compliance with the aims and provisions of the Act. While its functions and powers are defined under Section 29, the Act also ought to provide a clear definition of its status, composition, and budget, as well as the remit of its members and how they are appointed.

Lastly, the Committee welcomes Section 30 of the Act which provides that bodies representing controllers may adopt professional codes of conduct with a view to guaranteeing and improving the conditions of operation of information systems. Such codes are to be registered with the supervisory body, which may refuse registration if it considers that a code fails to comply with the law.

Conclusion

In light of the above, the Consultative Committee considers that the Argentinian Act on data protection is in full compliance with the provisions of Convention 108. Accordingly, based on its analysis of the applicable data protection legislation, the Consultative Committee is of the opinion that the request from Argentina to be invited to accede to Convention 108 should be given a favourable response.

The Committee further recommends that the Republic of Argentina be invited to accede to the additional Protocol.