11081/02/EN/Final
WP 63

Opinion 4/2002 on the level of protection of personal data in Argentina

Adopted on 3 October 2002

OPINION OF THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA
set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

On the level of protection of personal data in Argentina

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and in particular Articles 29 and 30 paragraph 1 (b) thereof,

Having regard to the Rules of Procedure of the Working Party[2], and in particular Article 12 and 14 thereof,

Whereas:

(1) The Government of the Republic of Argentina requested[3] that the Commission find that Argentina ensures an adequate level of protection within the meaning of Article 25 of the Directive,

(2) The European Commission sought the Opinion of the Working Party in this regard,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION: ARGENTINEAN LAW ON DATA PROTECTION

The protection of personal data is regulated in Argentinean Law in different legal instruments. A distinction can be drawn between general and sectoral norms.

1.1. General norms

The general norms result from the combination of the Constitution, the Personal Data Protection Act No. 25.326 and the Regulation approved by Decree No. 1558/2001. Together they constitute a common legal regime providing for the protection of personal data.

---

1 OJ L 281, 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 Adopted by the Working Party at its third meeting held on 11.9.1996

3 Letter by the Ambassador of the Republic of Argentina before the European Union of 23 January 2002

- ***Argentinean Constitution***

The Argentinean Constitution provides for a special judicial remedy for the protection of personal data, known as "habeas data". This is a subspecies of the procedure enshrined in the Constitution for the protection of constitutional rights and therefore upgrades the protection of personal data to the category of fundamental right. In particular, Article 43.3 of the Argentinean Constitution provides that *"any person will be able to request this action [speaking of habeas data] to know the content of all the data pertaining to him or her and their usage, contained in public records or databanks, or in private ones, whose purpose is to provide reports. In case of falsehood of information or its use for discriminatory purposes, a person will be able to demand the deletion, correction, confidentiality or update of the date contained in the above records. This Article will not affect the secrecy of journalistic information sources."*

The Argentinean jurisprudence has recognised "habeas data" as a fundamental and directly applicable right.

- ***Personal Data Protection Act of 4 October 2000 (Act 25.326, hereinafter 'the Act')***

The Act develops and widens the Constitutional provisions. It contains provisions relating to general data protection principles, the rights of data subjects, the obligations of data controllers and data users, the supervisory authority or controlling body, sanctions and rules of procedure for the 'habeas data' judicial remedy.

- ***Regulation approved by Decree No. 1558/2001 of 3 December 2001 (hereinafter 'the Regulation')***

This Regulation introduces implementing rules for the enactment of the Act, completes its provisions and also clarifies points of the Act that may be subject to diverging interpretation.

These three legal instruments make up together the general rules of Argentinean Law in the field of data protection (hereinafter 'Argentinean Law').

Scope of the Argentinean Law

The Working Party has assessed the adequacy of the level of personal data protection provided together by the Argentinean Constitution, the Act 25.326 and by the Regulation approved by Decree No. 1588/2001. The present opinion is therefore limited to the scope of these norms and does not refer to situations which may not be covered by these legal instruments. In particular, the Working Party has taken into account the explanations and the assurances given by the Argentinean authorities as to how the provisions of the Constitution, the Act and the Regulation are to be interpreted and as to what situations fall within the scope of the Argentinean Law in data protection.

Substantive scope

The Working Party notes the explanations provided by the Argentinean authorities on this issue. According to these, the Argentinean Law on data protection covers the following situations:

i. With regard to the data controller

The Argentinean Law covers the protection of:

1) *Personal data recorded in data files, registers, databanks or other technical means, which are public*. The Working Party understands this meaning that the data controller is a public institution or body. This interpretation results clearly from Article 4.3 of the Constitution and Article 1 of the Act.

2) *Personal data recorded in data files, registers, databanks or other technical means which are private*

   a) *in so far as the personal data files, registers or databanks go beyond exclusively personal use*. The Working Party notes the explanations provided by the Argentinean authorities on this issue. According to these, any use likely to affect the rights of data subject should be considered as going beyond exclusively personal use;

   or

   b) even when personal data files, registers or databanks do not go beyond exclusively personal use, if they are intended for the assignment or transfer of personal data, irrespective of whether the circulation of the data or information produced is performed for payment or free of charge.

The Working Party understands that both a) and b) refer to situations where the data controller is a private entity, be it a natural or a legal person.

As far as private data files are concerned, the Working Party notes that both Article 43.3 of the Constitution and Article 1 of the Act refer to *'private data files, registers, databanks or other technical means for data processing, whose purpose is to provide reports'*. The same wording appears in other provisions of the Argentinean Act, such as Article 14 on the right of access, Article 21 on the obligation to register, Article 29 on the powers of the controlling body, Article 33 and 35 on the requirement for the 'habeas data' judicial remedy, and Article 46 on transitory provisions. However, the wide interpretation stated above results from a number of arguments brought forward by the Argentinean authorities:

- Article 1 of the Regulation provides for a legal interpretation of the Act. In particular, it legally defines the concept of "private data files, registers, data bases or data banks, whose purpose is to provide reports" as "*those which go beyond exclusively personal use and those which are intended for the assignment or*

transfer of personal data, irrespective of whether the circulation of the data or information produced is performed for payment or free of charge."

- Article 24 of the Act provides that "*private persons forming data banks, registers or files which are not intended for an exclusively personal use must be registered in accordance with the provisions of Article 21*." Article 21 of the act imposes the obligation to register private data files *whose purpose is to provide reports*. Article 24 would make no sense if the Act did not apply more widely than to data files whose purpose is to provide reports. These two Articles confirm the parallelism of the expressions "data files *whose purpose is to provide reports*" and "data files *[…] which are not intended for an exclusively personal use*", as the legal definition of Article 1 of the Regulation establishes (see first argument, above).

- On the other hand, it must be noted that both the Act and the Regulation contain provisions regarding the processing of health data (Article 8 of the Act) or direct marketing (Article 27 of the Act and of the Regulation), where the data files, albeit going beyond exclusively personal use, may not be created with the purpose of providing reports. Again, these provisions would be superfluous if only private data files for the purpose of providing reports were covered by the Act.

According to the Argentinean authorities, the broad interpretation stated above has been followed by the Argentinean courts[4].

ii. With regard to the data subject

The Argentinean Law covers the protection of both natural and legal persons with regard to the processing of personal data. Article 2 of the Act defines "data subject" 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 processing referred to in this Act*", and Article 1 of the Act provides that "*the provisions contained in this Act shall also apply, to the relevant extent, to data relating to legal entities."* The Working Party notes the explanations provided by the Argentinean authorities on this issue. According to these, the requirement of having a legal domicile or local offices of branches in Argentina only applies for legal persons to be considered as data subjects. It does not apply to natural persons, and therefore all natural persons are considered as data subjects and are protected by the Argentinean Law.

iii. With regard to the means of processing

The Argentinean Law covers the protection of personal data with regard to both manual and automatic processing. In particular, Article 2 of the Act defines "data processing" as "*systematic 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."*

[4] Civil Court of Appeal, "Mantovano c/ Banco Regional de Cuyo, 2000; Becker José c/ Banco de la provincia de Buenos Aires, 2002

iv. With regard to the purpose of the processing operations

The Working Party notes that the Argentinean Law has a general scope in this regard. Since no general provision defines the purpose of the data files which should be subject to the Law, the Working Party understands that in principle data files, registers and banks set up for any purpose are subject to the Law, except in those cases where a specific provision rules otherwise. The Working Party draws attention, however, to the following issues:

– Data processing for the purpose of national defence, public security or the prosecution of criminal offences

These operations are subject to the provisions of the Act. In these cases the general rules of the Act and the Regulation apply, without prejudice to the specific provisions of Article 23 of the Act as lex specialis, which re-iterates the purpose limitation principle.

– Data processing for journalistic purposes

Article 43.3 in fine of the Constitution provides that "*This Article will not affect the secrecy of sources in journalism*". Along the same lines, Article 1 of the Act states that "*in no case shall journalistic information sources or data bases be affected*".

The Working Party notes the explanations provided by the Argentinean authorities on this issue. According to these, this provision is intended to preserve the secrecy of journalistic information sources as a necessary condition for safeguarding the fundamental right of freedom of the press, which is an important pillar of a democratic State. In that sense, the identity of the journalistic information source should be protected, for example against the request from a data subject for access to his personal data, which might include the information on the source of such data (cfr. Article 14 of the Regulation). On the other hand, the rectification of incorrect data published by the media should follow the rules of the right to get rectification linked to the freedom of the press.

The Working Party notes the explanations provided by the Argentinean authorities on this issue. According to these, this exception is to be applied in a restrictive way and does not cover personal data files which do not have journalistic purpose, even though the controller may carry out a journalistic activity (such as the human resources database of a newspaper).

– Data processing for statistical purposes

Article 28 of the Act provides as follows:

"1.- The regulations contained in this Act shall not apply to opinion polls, surveys or statistics collected pursuant to Law No. 17,622, market research works, scientific or medical research, and other similar activities, to the extent that the data collected cannot be attributed to a certain or ascertainable person.
2.- If in the data collection process it were not possible to keep the anonymity of the relevant person, a dissociation technique shall be used, so that no particular person may be identified."

The Working Party notes that this is not so much an exception to the general scope of the Law, but an application of the principle that the Law protects personal data, which are defined in Article 2 of the Act as *"information of any kind referred to identified or identifiable natural persons or legal entities"*. Therefore, the Working Party understands that when the data subject are identified or identifiable natural or legal persons, the Law fully applies, and that this justifies the provision of Article 28 of the Regulation, stating that *"Liability shall be borne by, and the fines provided for in Article 31 of Law No. 25 326 shall be applicable to, the records, registers, databases or databanks mentioned in Article 28 thereof in the event of any breach of its provisions."*

Territorial scope

This matter is regulated in Article 44 of the Act. Accordingly, the following distinction may be drawn:

I. Provisions of the Act which uniformly apply throughout the whole of the Nation:

- Chapter I: General provisions
- Chapter II: General data protection principles
- Chapter III: Rights of the data subjects
- Chapter IV: [obligations of] data controllers and data users of data files, registers and databanks
- Article 32: criminal sanctions
- The existence and main features of the 'habeas data' judicial remedy (as established in the Constitution)

II. Provisions of the Act which do not apply uniformly throughout the whole of the Nation:

- Chapter V: Control (supervisory authority)
- Chapter VI: Sanctions (which may be imposed by the supervisory authority)
- Chapter VII: Judicial remedy for the protection of personal data ('habeas data'): Rules of procedure

The Working Party notes the explanations provided by the Argentinean authorities on this issue. According to these, for these matters, the following rules apply:

– For registers, data files, data bases or databanks which are interconnected through networks at inter-jurisdictional (meaning "interprovincial"), national or international level: These cases are considered as falling within federal jurisdiction and thus subject to the provisions of the Act.
– For other kinds of registers, data files, databases or data banks: These cases should be regarded as falling under provincial jurisdiction. The provinces may issue legal provisions in these matters. To date, some of the provinces have already issued norms on procedure for the 'habeas data' remedy.

1.2. Sectoral norms

Data protection provisions are contained in a number of legal instruments regulating different sectors, such as credit card transactions, statistics, banking or health.

2. ASSESSMENT OF THE ARGENTINEAN LAW AS PROVIDING ADEQUATE PROTECTION OF PERSONAL DATA

The Working Party points out that its assessment on the adequacy of the Argentinean Law on data protection focuses on the **general norms** in this field, which are mentioned in the previous heading.

These provisions have been compared with the main provisions of the Directive, taking into account the Working Party's opinion on "Transfers of personal data to third countries; Applying Articles 25 and 26 of the EU data protection Directive[5]". This opinion lists a number of principles which constitute *a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate*. The result of this analysis is as follows:

2.1. Content Principles

Basic principles

- **the purpose limitation principle -** data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.

The Working Party understands that Argentinean Law complies with this principle. In particular, Article 4.3 of the Act sets out that "*the data which are processed shall not be used for any purpose or purposes which are different from or incompatible with those giving rise to their collection."*

- **the data quality and proportionality principle -** data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

The Working Party understands that this principle is complied with by Argentinean Law. In particular, Article 4.4 and 4.5 of the Act provide that *"the data shall be accurate and updated, if necessary. Any data totally or partially inaccurate, or incomplete, must be suppressed and replaced, or, as the case may be, completed, by the controller of the file or data base upon notification of the inaccuracy or incompleteness of the relevant information, without prejudice to the data subject's rights set forth in Section 16 of this Act"*. Further, Article 4.1 of the Act sets out that *"the 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 collected"*.

---

[5] WP 12 – Adopted by the Working Party on 24 July 1998, available at: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

- **the transparency principle -** individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the directive**.**

The Working Party understands that this principle is complied with by Argentinean Law. In particular, Article 6 of the Act provides as follows:

"Whenever personal data are obtained, data subjects shall be previously notified in an explicit and clear manner :
a) The purpose for which the data shall be processed, and who their addressees or type of addressees may be;
b) The existence of the relevant data file, register or bank, whether electronic or otherwise, and the identity and domicile of the person responsible therefore;
c) The compulsory or discretionary character of the answers to the questionnaire the person is presented with, particularly, in relation to the data connected with in the following Section;
d) The consequences of providing the data, of refusing to provide such data or of their inaccuracy;
e) The possibility the party concerned has to exercise the right of data access, rectification and suppression."

The Working party notes the explanations provided by the Argentinean authorities on this issue. According to these, a distinction should be drawn between the source of lawfulness of the processing and the obligation to inform the data subject.

On the one hand, the processing may be based on different legitimate grounds, which are listed in particular in Article 5. Such grounds include, inter alia, the consent of the data subject, the existence of a publicly available source, the execution of a public interest task, a legal obligation or a contractual relationship. It is understood, in accordance with Article 5 of the Regulation, that when the processing takes place with the data subject's consent, this consent must be an informed one and this means that all the information referred to in Article 6 of the Act must have been provided to the data subject beforehand.

On the other hand, Article 6 of the Act provides that "whenever personal data are obtained, data subjects shall be previously informed in an explicit and clear manner about: [there follows a list of items on the processing]". Although the wording of this Article may suggest that the obligation to inform the data subject refers to cases where the data are provided by the data subjects themselves and with their consent, the Argentinean authorities point out that such obligation is absolute, unconditioned, and does not depend on the ground of lawfulness for the processing. The obligation to inform applies in all cases, regardless that the personal data are requested from the data subjects or from third parties, and regardless that the processing takes place on the basis of the data subject's consent or of other legitimate ground out of those mentioned in Article 5 of the Act. Therefore, even when processing takes place without the data subject's consent, the obligation to inform the data subject still applies on the basis of Article 6 of the Act.

- **the security principle** - technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

The Working Party understands that Argentinean Law complies with this principle. In particular, Article 9 of the Act provides as follows:

"1. - The controller or the user of data files must take such technical and organisational measures as are necessary to guarantee the security and confidentiality of personal data, in order to avoid their alteration, loss, unauthorised consultation or processing, and which allow for the detection of any intentional or unintentional distortion of such information, whether the risks arise from human conduct or the technical means used.
2. - It is prohibited to record personal data in files, registers or banks that do not meet the requirements of technical integrity and security."

- **the rights of access, rectification and opposition -** the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.

As for the right of access, the Working Party understands that this principle is complied with by Argentinean Law. In particular, Article 14.1 of the Act provides that "*data subjects, once they have duly evidenced their identity, have the right to request and obtain information on their personal data included in public data registers or banks, or in private registers or banks intended for the provision of reports.*" This principle is further developed in the other paragraphs of Article 14 and 15 of the Act, and in Articles 14 and 15 of the Regulation.

As for the right of rectification and opposition, the Working Party understands that this principle is complied with by Argentinean Law. In particular, Article 16.1 of the Act provides that *"every person has the right to rectify, update, and when applicable, suppress or keep confidential his or her personal data included in a data bank."* This principle is further developed in the other paragraphs of Article 16 of the Act, and in Article 16 of the Regulation.

The exceptions to these rights are contained in Article 17 of the Act, allowing for restrictions only in the case of public data banks and for a limited list of important grounds, such as national defence, public order, and safety grounds or the protection of rights and interests of third parties, and also when such information could hinder pending judicial or administrative proceedings relating to the compliance with tax or social security obligations, the performance of health and environment control functions, the investigation of crimes and the verification of administrative violations. The Working Party considers that these exceptions are in line with the provisions of Article 13 of the Directive.

- **restrictions on onward transfers -** further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording

an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive.

The Working Party understands that this principle is broadly complied with by Argentinean Law. In particular, Article 12.1 of the Act provides *"the transfer of any type of personal data to countries or international or supranational entities which do not provide adequate levels of protection, is prohibited"*.

The exceptions to this principle are contained in Article 12.1 of the Act for the following cases:

"a) international judicial co-operation;
b) exchange of medical information, when so required for the treatment of the party affected, or in case of an epidemiological survey, provided that it is conducted in pursuance of the terms of Paragraph e) of the foregoing Section;
c) stock exchange or banking transfers, to the extent thereof, and in pursuance of the applicable laws;
d) when the transfer is arranged within the framework of international treaties which the Argentine Republic is a signatory to;
e) when the transfer is made for international co-operation purposes between intelligence agencies in the fight against organised crime, terrorism and drug-trafficking."

Article 12 of the Regulation has added to the list of exceptions the explicit consent of the data subject to the transfer, and the transfer from a public register in the same conditions as consultation, along the lines of Article 26.1(f) of the Directive.

The Working Party considers that these exceptions are broader than those provided for under the Directive, in particular, the exceptions contained in article 12.1 litterae b, c and d. The Working party finds this regrettable and would welcome some narrowing of the exceptions. It encourages the Argentinean Government to work toward this goal.

Additional principles to be applied to specific types of processing are:

- **sensitive data** - where 'sensitive' categories of data are involved (those listed in Article 8 of the directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

The Working Party understands that this principle is complied with by Argentinean Law. In particular, Article 2 of the Act defines "sensitive data" as *"personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labour union membership, and information concerning health conditions or sexual habits or behaviour"*. Article 7 of the Act provides for additional safeguards for their processing, as follows:

"1.- No person can be compelled to provide sensitive data.
2.- Sensitive data can be collected and subject to processing only in case there exist circumstances of general interest authorised by law. They may also be processed for statistical or scientific purposes provided data subjects cannot be identified.
3.- It is prohibited to create files, banks or registers storing information that directly or indirectly reveals sensitive data. Without prejudice to the foregoing, the Catholic

Church, religious associations, and political and labour organisations shall be entitled to keep a register of their members.
4.- Data referring to records on criminal or other offences can be processed only by the competent public authorities, within the framework established by the corresponding laws and regulations."
Further, Article 8 of the Act provides *that "public or private health institutions, as well as medical science professionals are entitled to collect and process such personal data as they relate to the physical or mental condition of patients who make use of their services or who are or may have been in their care, in pursuance of the principles of professional secrecy*."

- **direct marketing** - where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.

The Working Party understands that this principle is complied with by the Argentinean Law. In particular, Article 27 of the Act provides as follows:

"1.- Data suitable to establish certain profiles with promotional, commercial or advertising purposes may be processed in the collection of domiciles, distribution of documents, advertising or direct sales and other similar activities. This shall also include data, which permit to determine consumption habits, when such data appear on documents, which are accessible to the public or have been provided by the subjects themselves or have been obtained with their consent.
2.- In the instances contemplated in this Section, the data subject may exercise the right of access free of any charge.
3.- The data subject may at any time request the withdrawal or blocking of his name from any of the data banks referred to in this Section."

- **automated individual decision** - where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

The Working Party understands that this principle is complied with by Argentinean Law as regards processing operations by the public sector, since such automatic decisions are prohibited. In particular, Article 20 of the Act provides as follows:
"1.- Those judicial decisions or administrative acts involving an appreciation or assessment of human behaviour shall not have as their only basis the result of the computerised processing of personal data providing a definition of the profile or personality of the party concerned.
2.- Any act contrary to the preceding provision shall be irremediably null."

As for the private sector, the Working Party notes that no provision of Argentinean Law refers to this point. However, the Working Party recalls that an adequacy finding has to take into account all circumstances surrounding the transfer of personal data, and that the degree of risks that the transfer poses to the data subject is an important element in those "circumstances". The Argentinean Law does provide for safeguards for the data subject with regard to the provision of credit information services, which is a prominent sector where automated individual decisions are taken. Such safeguards are contained in Article 26 of the Act and of the Regulation and they limit the sort of data that can be processed, the source of the data and the period of time to

which they may refer. Therefore, the Working Party considers that the lack of a general provision concerning automated individual decisions for the private sector should not be an obstacle for an adequacy finding.

2.2. Procedural/ Enforcement mechanisms

The Working Party's opinion of 1998 indicates that the assessment of the adequacy of a third country's legal system should identify the underlying objectives of a data protection procedural system, and on this basis judge the variety of different judicial and non-judicial procedural mechanisms used in third countries.

With that regard, the objectives of a data protection system are essentially threefold:

– to deliver a good level of compliance with the rules;
– to provide support and help to individual data subjects in the exercise of their rights;
– to provide appropriate redress to the injured party where rules are not complied with.

- **to deliver a good level of compliance with the rules -** A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

The Working Party understands that the Argentinean Law has put in place a number of elements to serve this objective. In particular:

(a) Effective dissuasive sanctions

The Argentinean Law provides for a number of sanctions of different types and degrees according to the seriousness of the offence incurred by the controllers or users of the databases. Two sorts of sanctions can be identified:

i. Administrative sanctions

These sanctions are regulated in Article 31 of the Act and of the Regulation. They may include a warning, suspension, a fine ranging between one thousand pesos ($1,000.-) and one hundred thousand pesos ($100,000.-), closure or cancellation of the file, register or database. These sanctions may be imposed by the data protection supervisory authority and they may be graduated according to the nature of the personal rights affected, the volume of processing carried out, the benefits obtained, the degree of intent, the repetition of an offence, injury and damage caused to those concerned and to third parties, and any other circumstance of relevance in determining the degree of illegality and culpability concerned in the specific violation.

In addition, the controller or user of a public database may incur an administrative responsibility on the basis of the general rules on public service.

ii. Criminal sanctions

The Argentinean Criminal Code considers as a criminal offence knowingly to process false personal data and the breach of confidentiality or of data security. The Code provides for imprisonment penalties from 3 to 6 years (or from 4 years and a half to 9 years in case of harm to any person) and disqualification to hold public office for civil servants.

The Working Party understands that these are effective dissuasive sanctions, which may satisfactorily serve as a deterrent against unlawful processing of personal data.

(b) Data Protection Supervisory authority

The Argentinean Law provides for the establishment of a data protection controlling body. According to Article 29 of the Act, this controlling body is in charge or taking all actions necessary for the compliance with the objectives and other provisions of the Act. To such purposes, the body shall fulfil a number of functions, including assistance and advisory functions, to adopt rules and implementing provisions of the Act, keep a register data files and to control the compliance of data files with the Law. The body is endowed with a number of powers, such as that of requesting judicial authorisation to access data processing premises and equipment, requesting information from public and private entities, imposing administrative sanctions, engaging in criminal proceedings as accuser, and checking that the requirements and safeguards necessary for the inscriptions of private files are complied with.

Pursuant to Article 29 of the Regulation, the National Directorate for the Protection of Personal Data (DNPDP) has been established as the controlling body. This Directorate is part of the Ministry of Justice and Human Rights. The Director shall exercise his functions with full independence and he shall not be subject to instructions. His decisions can be appealed through the courts, according to the general rules on administrative procedures.

However, the Working Party draws attention to the fact that the head of the data protection supervisory authority is nominated and may be dismissed by the Minister of Justice and Human Rights, who also decides on the staffing of the authority. The authority is integrated within the structure of the Ministry of Justice. The Working Party considers that this situation does not guarantee that the authority may act in complete independence, and therefore urges that the necessary elements for that purpose be put in place, including changed modalities for appointment and dismissal of the head of the authority.

On the basis of Article 44 of the Act , the Working Party understands that the DNPDP may be considered as “federal jurisdiction’” and that it will therefore be responsible for the monitoring of data registers, files, or banks interconnected via national or international interjurisdictional networks. In other cases, such data registers, files or banks would fall under provincial jurisdiction and therefore fall outside of the competence of the DNPNP. The Working Party would welcome the establishment of data protection supervisory authorities in all provinces. This is important to ensure that there exists in all cases a system of direct verification by authorities and an

institutional mechanism allowing for independent investigation complaints other than the judiciary.

In the view of these considerations, the Working Party understands that Argentinean Law contains the elements necessary to deliver a good level of compliance with the rules.

- **to provide support and help to individual data subjects in the exercise of their rights -** The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

The Working Party notes that the Argentinean Law has put in place a number of elements to serve this objective. In particular:

(a) Habeas data judicial remedy

As mentioned above, the Argentinean Constitution provides for a special judicial remedy for the protection of personal data, known as "habeas data". This is a subspecies of the procedure enshrined in the Constitution for the protection of constitutional rights and therefore upgrades the protection of personal data to the category of fundamental right. In particular, Article 43.3 of the Argentinean Constitution provides that *"any person will be able to request this action [speaking of habeas data] to know the content of all the data pertaining to him or her and their usage, contained in public records or databanks, or in private ones, whose purpose is to provide reports. In case of falsehood of information or its use for discriminative purposes, a person will be able to demand the deletion, correction, confidentiality or update of the date contained in the above records. This Article will not affect the secrecy of journalistic information sources."*

The legislative provisions enacting this Constitutional remedy are contained in Articles 33 to 43 of the Act. The "habeas data" is thus shaped as a simplified and quick judicial remedy. It can be used by data subjects against controllers or users of the data files. The Argentinean Government has clarified that, in accordance with what has been said with regard to the scope of the data protection in Argentinean Law, this remedy may be used against the controllers or users of any public data base and of any private data base (and not only private data bases whose purpose is to provide reports), as long as they go beyond exclusively personal use. This point has been confirmed by court rulings in this sense.

The Working Party notes the explanations provided by the Argentinean authorities on this issue. According to them, the Act widens the scope of the Constitutional provision, allowing for this remedy to be used in those cases in which is presumed the processing of personal data whose registration is forbidden in the Act. This means that any breach of the data protection rules can allow for the 'habeas data' to be used.

The Working Party further notes that the burden of proof is laid upon the data controller or user in case an exception to the right of access, rectification or deletion is alleged.
The 'habeas data' remedy allows for a court ruling imposing that the information be suppressed, rectified, updated or declared confidential. The Working Party

acknowledges that the court ruling is to be communicated to the controlling body, and that this may allow for the enforcement by the DNPDP within its competence of the data protection rules with regard to other data subjects concerned who may not have been a party in the original 'habeas data' procedure.

(b) General judicial remedies

Besides 'habeas data', the general rules in Argentinean Law allow for the data protection rights and obligations to be enforced through the courts according to the general procedures. In particular, a court proceeding may be initiated by the data subject before a civil court for compensation of the damage suffered or for enactment of any of the rights recognised by the Act or the Regulation. Further, criminal proceedings may be initiated for the criminal offences with regard to the processing of personal data included in the criminal Code.

In the view of these considerations, the Working Party understands that Argentinean Law contains the elements necessary to provide support and help to individual data subjects in the exercise of their rights.

- **to provide appropriate redress to the injured party where rules are not complied with** - This is a key element, which must involve a system of independent adjudication, or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

The Working Party points out that neither the Act nor the Regulation contain specific rules on the right of any person who has suffered damage as a result of an unlawful processing operation to receive compensation for the damage suffered. In this regard the Working Party notes the explanations provided by the Argentinean authorities on this issue. According to these, in the absence of special rules, the general rules in Argentinean Law on liability apply. Depending on the case, the provisions to apply may be those of contractual liability (where the processing takes place in the framework of a contractual relationship between the parties) or those of extra-contractual liability in other cases. The Argentinean rules in both cases are in line with the European tradition in Civil Law and follow the principle that requires that damage be compensated in case of unlawful handling.

In the view of these considerations, the Working Party understands that that Argentinean Law contains the elements necessary to provide appropriate redress to the injured party where rules are not complied with.

2.3. Other issues

The Working Party notes that Article 5 of the Argentinean Act allows for personal data to be processed without the data subject's consent when the data are obtained from sources subject to unrestricted public access. The Working Party draws the attention to the need for rules that guarantee that the data included in a source subject to unrestricted public access are of such nature that their processing without the data subject's consent is not likely to constitute a threat to the fundamental rights and freedoms of the individuals, and in particular to their right to privacy. It is understood that even in the case of personal data included in a source subject to unrestricted public access all the provisions of the Argentinean data protection Law apply.

3. RESULTS OF THE ASSESSMENT

The Working Party stresses that, in order to carry out the present assessment on the Argentinean Law, the Argentinean Government has provided information on how the provisions of the Argentinean Constitution, the Act and the Regulation are to be interpreted, and has given assurances that the Argentinean data protection rules are being implemented along such interpretation. The Working Party has therefore based its analysis upon such information and assurances of the Argentinean Government, and this opinion is thus dependent on these elements provided by the Argentinean Government being confirmed in the actual implementation of the data protection rules in Argentina. In particular, as regards the scope of the Argentinean Law, the Working Party has taken into account the explanations and the assurances given by the Argentinean authorities as to how the provisions of the Constitution, the Act and the Regulation are to be interpreted and as to what situations fall within the scope of the Argentinean Law in data protection. The present opinion has been drafted on the basis of these assumptions and explanations and in the absence of any substantial experience with the practical application of the legislation, both at federal or provincial level. This is also the case as regards the effective taking into consideration by the Argentinean Authorities, within a reasonable period of time, of the reservations expressed here above, and of the requests for the improvement or amendment of the existing legal texts.

In conclusion, on the basis of the above mentioned findings, the Working Party assumes that Argentina ensures an adequate level of protection within the meaning of Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data an on the free movement of such data.

However, the Working Party also encourages the Argentinean authorities to take the necessary steps to overcome some remaining weaknesses in the present legal instruments, as identified in this opinion and requests the Commission to continue the dialogue with the Argentinean Government with that purpose. In particular, the Working Party urges the Argentinean Authorities to ensure the effective enforcement of the legislation at provincial level by means of the creation of the necessary independent control authorities where they do not exist yet and, in the meantime, to look for appropriate temporary solutions in accordance with the Argentinean constitutional order.

Done at Brussels, 3 October 2002

For the Working Party
The Chairman
Stefano RODOTA