ARTICLE 29 DATA PROTECTION WORKING PARTY

0475/10/EN
WP 177

Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay

Adopted on 12 October 2010

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No LX-46 01/190.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

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, and in particular Articles 29 and 30 paragraph 1 (b) thereof,

Having regard to the Rules of Procedure of the Working Party, and in particular Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

On 20 October 2008 the Mission of the Eastern Republic of Uruguay (thereafter "Uruguay") to the European Union sent a letter to the European Commission to transmit the official request of the Uruguayan Government to initiate the procedure to declare that Uruguay provides an adequate level of protection with regard to transfers of personal data from the EU/EEA, pursuant to Article 25(6) of Directive 95/46/EC on the protection of personal data ("the Directive").

In order to proceed with studying whether Uruguay provides an adequate level of protection, the Commission requested a report from the *Centre de Recherches Informatique et Droit* (CRID) of the University of Namur. This lengthy report analysed the degree to which the Uruguayan legal system complies with requirements in terms of substantive legislation and the implementation of mechanisms to apply regulations protecting personal data, set out in the working paper "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive", approved by the Working Party created in relation to Article 29 of the Directive on 24 July 1998 (document WP12). The Uruguayan authorities, via the Unit for the Regulation and Control of Personal Data (URCDP) made comments in answer to the issues arising in this report, by agreement of the Executive Council of the URCDP on 11 February 2010.

Said report, together with the comments from the Uruguayan authorities were assessed by a Sub-Group set up specifically for this purpose within the Article 29 Working Party, which submitted for appraisal by the Working Party the sending of a letter by its Chairman to the Uruguayan authorities, in which, after giving a positive appraisal of the data protection regime in Uruguay (included fundamentally in Law No. 18,331, of 11 August, on the Protection of Personal Data and "Habeas Data" Action -LPDP, after its initials in Spanish-, and the Regulating Decree of 31 August 2009, dictated on its development –DPDP-), said authorities were notified of those issues which could require further clarification.

The Uruguayan authorities, by means of the URCDP, sent the Article 29 Working Party a lengthy report, approved by agreement of its Executive Council of 23 June 2010, giving its responses to the questions raised in this letter. They also provided a range of

documentation on the situation regarding data protection in the country, including this body's annual report for 2009 and its activity report up to 31 May 2010, various resolutions passed by its Executive Council, and relevant legal resolutions on the issue of personal data protection.

This report was redistributed in September 2010 to the members of the Sub-Group, who analysed it, with particular focus on the issues raised in the letter sent by the Working Party to the Uruguayan authorities. Having analysed the aforementioned information, the Sub-Group deems it possible to submit the present document to the Working Party without further delay.

2. LEGISLATION ON DATA PROTECTION IN URUGUAY

The Political Constitution of the Eastern Republic of Uruguay, passed in 1967, does not expressly acknowledge the rights to privacy and the protection of personal data. However, this Supreme Law is not specifically exact on this matter, given that its Article 72 provides that "The listing of rights, obligations and guarantees made by the Constitution does not exclude others that are inherent to the human personality or that derive from the republican form of government."

Furthermore, Article 332 of the Constitution states that "The application of the precepts of this Constitution that acknowledge individuals' rights, as well as those awarding rights and imposing obligations on public authorities, should not be impeded by the lack of pertinent regulations, but rather this will be substituted through recourse to the underlying bases of similar laws, to the principles of law and generally accepted doctrines."

The Working Party thus confirms that these two open clauses acknowledge the existence of the individual's fundamental rights not expressly acknowledged in the Uruguayan Constitution. This conclusion is reiterated if account is taken of the fact that Article 1 of Law 18,331, on the Protection of Personal Data and "Habeas Data" Action (LPDP) states with absolute clarity that "The right to the protection of personal data is inherent to the human being, so it is included in Article 72 of the Constitution of the Republic."

By virtue of the aforementioned, the fundamental right to the protection of personal data, acknowledged as such by the Uruguayan legislative system, is regulated by the LPDP, which was proclaimed on 11 August 2008, replacing the previous Law on the Protection of Personal Data to be used in Commercial Reports and "Habeas Data" Action, passed in 2004, and which is now wholly responsible for regulating this matter within all sectors of activity. Hence, its Article 3 lays down as a general principle that "The regulations of this law shall be applied to personal data recorded in any medium that makes them likely to be processed, and to any kind of subsequent use to which these data may be put by the public or private sectors."

Subsequently, in developing the provisions of the aforementioned LPDP, the Executive Government of the Republic passed the Regulating Decree developing this law (DPDP), of 31 August 2009. The Preamble of this provision points out that "it is appropriate to adjust the national legal system on this matter to the most accepted comparable legal

regime, essentially that established by European countries through 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."

This Decree introduces some clarifications and regulatory developments with regard to a range of provisions in the LPDP. In particular, the Group considers it necessary to make reference to those relating to the territorial scope of application of the LPDP, security, the exercising of rights to access, update, include and remove data, and the detailed regulation of the organisation, powers and functioning of the Control Body, called the Unit for the Regulation and Control of Personal Data (URCDP).

Lastly, the Party wishes to stress that the documentation sent by the Uruguayan authorities in response to the letter it sent them includes the agreement of the Executive Council of the URCDP whereby it rules "*To work to ensure the Ministry of Foreign Relations initiates the necessary proceedings with the Council of Europe for the purposes indicated in this resolution, in accordance with Art. 23 of Convention 108 of the Council of Europe (Strasbourg Convention) and its Additional Protocol of 28 January 1981, for the Protection of Individuals with regard to Automatic Processing of Personal Data.*"

3. ASSESSMENT OF THE LEVEL OF ADEQUACY OF THE PERSONAL DATA PROTECTION AFFORDED BY DATA PROTECTION LEGISLATION IN URUGUAY

The Working Party indicates that its assessment of the adequacy of the legislation on the protection of personal data in force in Uruguay refers fundamentally to Law No. 18,331, of 13 August, on the Protection of Personal Data and "Habeas Data" Action (LPDP) and the Regulating Decree of 31 August, passed in relation to this law (DPDP).

The precepts of this Law have been compared with the main provisions of the Directive, taking account of the report by Working Party WP12. This report sets out a series of principles that constitute a "*nucleus*" *of* "*content*" *principles for data protection and of* "*procedure/application*" *requirements, compliance with which could be considered a minimum requirement for considering the protection to be adequate.*

3.1 Scope of application of the legislation

From an objective point of view, as has been indicated, Article 3 of the LPDP, reproduced by Article 2 of the DPDP, establishes the principle that this regulatory regime "will be applied to personal data recorded in any kind of medium that makes them likely to be processed, and any kind of subsequent use of these data within the public or private domains." At the same time, the data protection regulations will, in compliance with Article 2, be applicable by extension to legal persons, where relevant.

The Working Party welcomes the clarifications offered by the Uruguayan authorities in response to the concerns expressed by the Party regarding the Law not being applicable to "databases created and regulated by special laws."

On this issue, the Uruguayan authorities have responded that the special laws cited, of which they have provided a range of examples, lay down a more demanding data protection system than that contained in the General Law which, in any case, will always be additionally applied in relation to issues that are not governed by specific legislation, in application of the previously cited Article 322 of the Constitution of the Republic.

On the scope of territorial application of the law, the Working Party has indicated its satisfaction that the DPDP expressly contains an article referring to this issue, which is fundamentally the same as the regime established in Article 4 of the Directive, which implies a guarantee of compliance with the principles and, in particular, with the one on limitation of subsequent transfers.

Thus, the aforementioned Article 3 considers that the processing of personal data is subject to the LPDP when:

- They are performed by database or processing controllers established in Uruguay, who carry out their activities there, whatever their legal form.

- The database or processing controller is not established in Uruguay, but processes the data by means of media located within the country.

Furthermore, it adds that an exception is made for this second rule “in cases in which the aforementioned media are exclusively used for transfer purposes, as long as the database or processing controller appoints a representative with domicile and permanent residence in the national territory before the Control Entity so as to comply with the legal obligations being regulated and in this regulation".

Therefore, in relation to the previously mentioned clarifications, the Working Party considers the scope of application of the Uruguayan legislation on data protection to be similar to that established by the Directive.

3.2. Content principles

a) Essential principles

1) The purpose limitation principle: The data should be processed for a specific purpose and subsequently used or transferred only where this is not incompatible with the purpose of the transfer. The only exceptions to this rule would be those necessary in a democratic society for one of the reasons described in Article 13 of the Directive.

The Working Party is pleased to verify that this principle is expressly contained in the LPDP, Article 5 c, which expressly establishes that the actions of database controllers, both public and private and, in general, those who act in relation to the personal data of third parties, should comply with the principle of purpose limitation.

Article 6 of the Law states that “No database may be used to violate human rights, nor to be contrary to laws or public morals.” While Article 8 adds that “The data subject to processing shall not be used for any purposes other than or incompatible with the reasons for which they were gathered.”

The only exception to this precept is that “The regulations shall determine cases and procedures in which, exceptionally, and in relation to their historical, statistical or scientific value and in line with specific legislation, personal data can be kept even if there is no current need or relevance for doing so.” Article 37 of the DPDP regulates the procedure for authorising data conservation for historical, statistical or scientific purposes. The Working Party understands that this exception is similar to that established under Article 6.1 b) of the Directive.

Likewise, Article 11 of the LPDP indicates that “ Natural or legal persons that lawfully obtain information from a database that carries out processing are obliged to use it in such a way that maintains its confidentiality, and exclusively for the usual operations of their business or activity, with any dissemination of said information to third parties being prohibited.”

Therefore, the Working Party considers that Uruguayan legislation complies with this principle.

> **2) The data quality and proportionality principle:** Data should be accurate and, where necessary, kept up to date. The data should be appropriate, relevant and not excessive in relation to the purpose for which it is transferred or subsequently processed.

In the Working Party's opinion, this principle appears to be regulated by Article 7 of the LPDP by the so-called “veracity principle”, listed among the main guiding principles of the Law in Article 5 b) therein.

The aforementioned Article 7 establishes that “Personal data collected for processing purposes shall be truthful, appropriate, impartial and not excessive in relation to the purposes for which they were obtained. Data collection shall not be carried out through unfair, fraudulent, abusive, extortive means or in any way contrary to the provisions of this Law.

Furthermore, the LPDP requires that “Data shall be accurate and updated, where necessary”, adding that “Whenever data is shown to be inaccurate or false, the controller shall delete, complete or replace them with accurate, truthful and updated data, as soon as he/she/it becomes aware of the situation, . In addition, any expired data shall be deleted according to the provisions of this law.”

Lastly, Article 8 of the LPDP states that “Data shall be deleted whenever they cease to be necessary or relevant for the purposes for which they were collected.”

The Working Party also takes into consideration the Uruguayan authorities' explanations on the supposition of processing legitimacy referred to in Article 9 c) of the LPDP, which states that “Previous consent shall not be required when (...) these are lists with data regarding natural persons limited to names and surnames, identity card

number, nationality, address and birth date. In the case of legal persons, the corresponding data are corporate name, brand name, single taxpayer number, address, phone number and identity of the people in charge."

On this issue, the Uruguayan authorities have clarified that the legitimisation offered by this precept may under no circumstances be understood to be different to the principles of legitimisation, proportionality and limitation of purpose. Hence, even when it is not necessary to obtain the consent of the person concerned, the controller can only process the data referred to in this article when such processing falls within the scope of the explicit and lawful purposes identified, and as long as the data mentioned is appropriate, relevant and not excessive in relation to the mentioned purposes, and there is no other legitimisation than necessary compliance with both principles.

In view of all the aforementioned, the Working Party considers that the principle of proportionality and data quality is also covered in Uruguayan legislation.

> **3) Principle of transparency:** Data subjects should be informed about the purpose for which the data are being processed and the identity of the processing controller in the third country, and any other aspect required to ensure fair treatment. The only exceptions allowed must be covered by Articles 11.23 and 13 of the Directive.

The Working Party considers that the obligation to inform the data subject about the processing of his/her data is covered by Article 13 of the LPDP, according to which data subjects should be previously expressly, accurately and unambiguously informed when their personal data are gathered:

- The purposes for which the data will be processed and the possible recipients or type of recipients.

- The existence of the database, electronic or of any other kind, and the identity and address of the controller.

- The compulsory or voluntary nature of the answers to the questionnaire sent, in particular with regard to sensitive data.

- The consequences of providing the data, failure to do so or giving inaccurate data.

- The data subject having the possibility to exercise his/her rights to access, rectify or erase data.

The Working Party likewise confirms that when the processing is based on the consent of the data subject, the latter will have to be informed, as is required in under Articles 9 of the LPDP and 5 of the DPDP, with this second article specifying that "When the data subject's consent is requested to collect and process his/her data, the latter should be informed in such a way that he/she is unequivocally aware of the purpose for which the data will be used and the type of activity undertaken by the database or processing controller. Otherwise, the consent will be null and void."

The Working Party likewise takes into consideration the clarifications provided by the Uruguayan authorities concerning the obligation to inform the data subject in all cases. Hence, although the wording of Article 13 could make it appear that the obligation to inform the data subject refers only to those cases in which the data subject provides the data voluntarily and with his/her consent, the Uruguayan authorities say this obligation is absolute, unconditional and does not depend on the reason legitimising the data processing. The obligation to inform the data subject applies in all cases, irrespective of whether the personal data is requested from the data subject or from a third party and whether the processing is carried out by virtue consent of the data subject or any other lawful reason.

Moreover, the Uruguayan authorities clarify that in the event of data having been obtained through a third party as the result of a data communication, the data subject would also have to have been previously informed about this transfer by the person or entity communicating the data, and of the recipients of this transferred data, in accordance with Article 13 of the LPDP.

> **4) Security principle:** The controller must adopt appropriate technical and organisational measures against the risks presented by the treatment. Any person acting under the authority of the controller, including the person in charge of processing, must not process data except on instructions from the controller.

The Working Party highlights that within the principles listed in Article 5 of the LPDP the principle of security is contained in letter e).

Article 10 of the Law develops this principle, stating that "The controller or user of the database must take all necessary measures to ensure the security and confidentiality of personal data. These measures aim to avoid the data being altered, lost, consulted or treated without authorisation, as well as to detect information being passed on, intentionally or not, whether these risks arise from human action or from the technical means used," and adds that "It is prohibited to record personal data in databases that do not meet technical integrity and security requirements."

Furthermore, Article 7 of the DPDP adds that "Both the controller and the person in charge of the database or processing must protect the personal data processed, by using the most suitable technical and organisational measures to ensure its integrity, confidentiality and availability," with the nature of the processor being the same as that defined by the Directive.

The Working Party also notes that Article 8 of the DPDP establishes the obligation to inform the individuals concerned about any possible security breaches that have occurred, stating that "When database controllers or processors become aware of security breaches having taken place at any stage of the processing being carried out, and which are likely to significantly affect the individual's rights, they should inform them of this event."

Finally, the Working Party looks at the regulation of the obligation to confidentiality and secrecy governed by Article 11 of the LPDP, considering that, based on the indications given, Uruguayan legislation complies with the safety principle according to the terms set out in the WP12 document.

5) Rights of access rectification and opposition: An individual must be entitled to a copy of all data relating to him or her, and the right to rectify any data that is inaccurate. In certain situations, the individual should also be able to oppose his or her data being processed. The only exceptions to these rights should be in line with Article 13 of the Directive.

In relation to the right of access, Article 14 of the LPDP provides that "Any personal data subject who has previously verified their identification through an identification document or respective power, is entitled to receive any information about him or herself held in public or private databases. This right of access can only be exercised free of charge every six months, unless it has provoked a legitimate interest in accordance with the legal system."

Such information "must be provided within five working days of being requested. If the period expires without the request being answered, or if it is denied for reasons not justified under this law, habeas data will be put into action." Furthermore, "The information must be provided clearly, free of coding and where necessary accompanied by an explanation, in language accessible to the average knowledge level of the population, expressed in commonly-used terms."

Article 14 also states that "Information should be comprehensive and cover the entire record relating to the person in question, even if the request only refers to one aspect of their personal data. In no case should the report reveal information relating to others, even when they are linked with the subject" and "the information may be provided in writing, by electronic means, by phone, image, or by other such suitable means, as the holder deems fit."

The Working Party takes into consideration the clarifications provided by the Uruguayan authorities to the effect that, notwithstanding the wording of Article 9 d) of the DPDP, the individual does not have to give any reasons for his or her request, with verification of his or her identity being sufficient for this purpose. In particular, the Working Party takes into consideration the URCDP Agreement of 18 June 2010 which states that "*in order to exercise the right of access established in article 14 of Act No. 18.331 on the Protection of Personal Data and Habeas Data writ, the database controller shall solely demand as a requirement for the request, the identification of the data holder"*.

In relation to the other rights of individuals, Article 15 of the LPDP states that "Every natural or legal person is entitled to request the correction, updating, inclusion or deletion of his or her personal data that is held in a database upon confirmation of an error, incorrect entry or exclusion in his or her information."

The Law adds that "The controller of the database or processor should proceed to rectify, update, include or delete such information, using whatever operations are necessary for this purpose, within no more than five working days from receiving the individual's request or, where appropriate, report the reasons why this is considered not to be applicable," concluding that "Failure on the part of the database controller or processor to comply with this obligation, or to do so by the deadline, will entitle the data subject to take recourse in the habeas data action provided for in this law."

The Working Party takes note of the clarifications made by the DPDP, focusing initially on the definitions laid down in Articles 10 to 12.

According to Article 10, the right to correction is defined as follows "The right to correction is the data subject's right to have any data that are inaccurate or incomplete changed." Article 11 defines the right to updating as follows "The right to updating is the data subject's right to have data that are inaccurate on the date on which the right is exercised changed" and Article 12 defines the right to inclusion as follows "the right to inclusion is the data subject's right to have his or her relevant information incorporated into a database when a justified interest is accredited."

Furthermore, Article 13 refers to the right to deletion as follows "the right to deletion is the data subject's right to remove data, the use of which by third parties is unlawful, or that proves to be inappropriate or excessive."

In relation to this law, the Working Party takes on the points indicated by the CRID in the two reports regarding the adequacy of data protection Uruguay, and in particular in the addenda relating to the implementation of the DPDP, considering that, through the regulation on the right to deletion, Uruguayan law recognises the right to opposition in the terms set out in Article 14 of the Directive.

In relation to exceptions to the exercise of these rights, the Working Party finds that those based on the need to preserve information for historical, statistical or scientific reasons and in accordance with applicable law, or as a result of the continuation of contractual relations between the controller and the data subject, which justify the processing of the data, are consistent with the principles of data protection.

Furthermore, the Working Party finds that the exceptions established in Article 26 of the LPDP that take into consideration "the dangers that could arise in relation to defence of the State or public safety, protection of the rights and freedoms of third parties or the needs of ongoing investigations" can be considered similar to those established in Article 13 of the Directive. In particular, the Working Party takes into account the fact that the Law itself provides in Article 26 that "Any data subject who is partially or fully denied exercise of the rights mentioned in the preceding paragraphs may notify the Control Body, which shall rule on the legality or illegality of the denial."

> **6) Restrictions on onward transfers to other countries:** Successive transfers of personal data from the third party destination country to another country may only be permitted if the latter also ensures an adequate level of protection. The only exceptions permitted should be those provided for in paragraph 1 of Article 26 of the Directive

The Working Party notes that Uruguayan law has defined a concept of international data transfer similar to that established by the Member States, given that this encompasses not only data transfers to a data controller located in another State, but also cases in which data is transmitted to a processor.

This is taken from the definitions of export and import of data established in letters e) and f) of Article 4 of the DPDP. An exporter is specifically defined as "a natural or legal person, public or private, located in Uruguayan territory who transfers personal data to

another country, in accordance with the provisions of this regulation" and an importer is "a natural or legal person, public or private, who receives data from another country, in an international transfer, whether he or she be controller, processor or third party."

Article 23 of the LPDP establishes as a general rule for transfers that "The transfer of any personal data to countries or international organisations that do not provide adequate levels of protection according to the standards of International or Regional Law is prohibited." The last two paragraphs of this article add that "Without prejudice to the stipulations of the first paragraph of this Article, the Regulatory and Control Unit for the Protection of Personal Data may authorise a transfer or a series of transfers of personal data to a third party country that does not ensure an adequate level of protection, if the controller offers adequate safeguards regarding the protection of privacy, the rights and freedoms of individuals, and the exercise of their respective rights. Such safeguards may result from appropriate contractual clauses."

Thus, the Working Party finds that these rules establish a regulatory system for international transfers of data similar to that set out in Articles 25.1 and 26.2 of the Directive.

Article 23 of the LPDP also goes on to provide two lists of exceptions to the authorisation. The Working Party finds that the second of these lists is the same as the exceptions established in Article 26.2 of the Directive, since it sets out the following cases that are excluded from the authorisation:

- When the individual has given his consent unambiguously to the proposed transfer.

- When the transfer is necessary for the execution of a contract between the individual and the controller or for the implementation of pre-contractual measures taken at the request of the individual.

- When the transfer is necessary for the conclusion or execution of a contract or for one yet to be signed in the interest of the individual, between the controller and a third party.

- When the transfer is necessary or legally required in order to safeguard an important public interest, or in order to recognise, exercise or defend a right in court proceedings.

- When the transfer is necessary to safeguard the individual's vital interests.

- When the transfer is made from a register which, by virtue of legal provisions or regulations, is intended to provide information to the public and is open to be consulted by the general public or by any person who can demonstrate a legitimate interest, provided that they fulfil, in every case, the legally-established requirements for doing so.

The Working Party further notes that the first list includes a list of assumptions that do not, however, literally coincide with those established in Article 26.1 of the Directive. On this list the following appear as exemptions from the authorisation:

a) International judicial cooperation, according to the relevant international instrument, be it a Treaty or a Convention, in accordance with the circumstances of the case.

b) Exchange of medical data, when it is required in order to treat the person in question for reasons of public health or hygiene.

c) Bank transfers or exchanges, with regard to the respective transactions, and in accordance with applicable law.

d) Agreements under international treaties to which the Eastern Republic of Uruguay is a party.

e) International cooperation between intelligence agencies to combat organised crime, terrorism or drug trafficking.

The Working Party draws attention to its report 4/2002 on the level of protection of personal data in Argentina, pointing out that the exceptions raised in the letters b), c) and d) could, on a first reading, suggest the existence of further exceptions than those set out in Article 26.1 of the Directive, which would affect the application of this principle.

However, the Working Party welcomes the clarifications provided by the Uruguayan authorities to clarify that these exemptions can not be understood to have any broader application than that established in Article 26.1.

Thus, the exception provided in paragraph c) relates to the existence of a contractual relationship between the individual and the exporter, which necessarily requires the international transfer of personal data in order to be implemented.

Exceptions b) and d) shall always be interpreted to concurrently consider the existence of an important public interest, the ratification of an international agreement binding on Uruguay, or public health issues within the general concept of "substantial public interest."

With this in mind, the Working Party accepts these explanations, but recommends the adoption of measures to ensure that the Uruguayan authorities use this interpretation of the regulations studied.

b) Additional principles

The WP12 document refers to certain principles that should be applied to specific types of processing, specifically the following:

> **1) Sensitive data:** In the case of "sensitive" data categories (those listed in Article 8 of the Directive), additional safeguards should be established, such as the requirement for individuals to give their explicit consent for data processing.

The Working Party considers that this principle is observed in Uruguayan data protection legislation.

Article 4 e) of the LPDP defines sensitive data as "personal data revealing racial or ethnic origin, political preferences, religious or moral beliefs, trade union membership or information concerning health or sex life." In particular, in relation to health data, Section 4 d) of the DPDP further clarifies the definition in terms similar to those established by the Court of Justice of the European Union, saying that sensitive data is "information concerning the past, present or future physical or mental health of a person," adding that " Among others, it includes data related to people's health such as their percentage of disability or genetic information."

Article 18 of the LPDP establishes the general principle that " No person can be compelled to provide sensitive data. It can only be processed with the express written consent of the data subject," and then continues by stating that "Sensitive data can be collected and processed for reasons of general interest authorised by law, or when the applicant organisation has legal mandate to do so. It may also be processed for statistical or scientific purposes when not in connection with the individual to whom it relates."

Article 19, in relation to health data, states that "Public or private health facilities and professionals linked to the health sciences may collect and process personal data relating to the physical or mental health of patients they attend or who are or have been under their treatment, as long as they respect the principles of confidentiality, specific regulations and the provisions of this law" and Article 17, in relation to the communication of health data, states that the consent of individuals may only be excepted in cases that "Concern personal health data and are necessary for reasons of public health and hygiene, emergencies or for epidemiological studies, while preserving the identity of the data subjects through proper disassociation mechanisms."

Furthermore, Article 19 prohibits "the formation of databases that store information that directly or indirectly reveal sensitive data. Exceptions are made for those owned by political parties, trade unions, churches, religious denominations, associations, foundations and other non-profit entities, for political, religious or philosophical purposes or those that are trade union-related or make reference to racial or ethnic origin, health or sexual life, with regard to the details of their partners or members, with the disclosure of such data always requiring the prior consent of the data subject."

> **2) Direct marketing:** Should the data transfer be for direct marketing purposes, the individual should be able to refuse to have his or her data used for this purpose at any time.

The Working Party considers that this principle is covered in Article 21 of the LPD, referring to the circumstances of "collection of home addresses, distribution of documents, advertising, sale or other similar activities."

Thus, after noting that "data that is suitable for establishing certain profiles for promotional, commercial or advertising purposes may be processed, or that makes it possible to establish consumer habits, if this data appears in documents accessible to the public or has been supplied by the individuals themselves or obtained with their

consent" and recognising the free exercise in all cases of the right to access, the last paragraph of the article states clearly that "The data subject may at any time request his or her data to be removed or blocked in the databases to which this article applies."

3) Automatic individual decision: When the objective of a transfer is to take an automatic decision, in the sense of article 15 of the Directive, the interested party must have the right to know the reasoning behind this decision, and other measures must be taken to protect the person's legitimate interests.

The Working Party confirms that this principle is expressly acknowledged by Article 16 of the DPL, which is based on the general rule that "People have the right to not be subject to a decision with legal impacts that may significantly affect them, based on the processing of data, whether automatic or not, that is intended to assess specific aspects of their personality, such as employment performance, credit, reliability or behaviour, among others."

Furthermore, the third paragraph of this article establishes a principle that is similar to the one indicated in document WP12, as it stipulates that "the person affected shall have the right to obtain information from the controller, both regarding the assessment criteria and the programme used for processing that was used to make the decision expressed".

3.3. Procedural/enforcement mechanisms

The WP12 Working Party Opinion "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" states that, in order to evaluate whether the legal systems of third countries provide adequate protection, it is necessary to distinguish the underlying objectives of a data protection regulation system, using this basis to judge the variety of different mechanisms of legal and non-legal procedures used in other countries.

In this respect, there are basically three objectives for a data protection system:

- To deliver a good level of compliance with regulations,
- To provide support and help to individual data subjects,
- To provide appropriate redress to those affected when regulations are not observed.

a) To deliver a good level of compliance with regulations: Generally, a good system is characterised by controllers who have a perfect understanding of their obligations and by individuals who know their rights and the ways in which they can exercise them. Effective sanctions and deterrents are important to guarantee that the regulations are observed, as are, naturally, systems of direct verification by the authorities, auditors and independent civil servants in charge of data protection.

The Working Party considers that this objective is fulfilled by different provisions contained in Uruguayan legislation, particularly the following:

The Unit for the Regulation and Control of Personal Data (URCDP)

The LPDP, by virtue of Article 31, created the control authority for data protection, called the "Unit for the Regulation and Control of Personal Data" (URCDP in Spanish) which is an "autonomous entity of the Agency for the Development of Electronic Government and the Knowledge-Based Society (AGESIC in Spanish). This autonomous entity has the very broadest technical autonomy".

AGESIC contains the autonomous entities, which are the aforementioned URCDP and the Unit for Access to Public Information (UAIP in Spanish).

The Working Party takes note of the Uruguayan authorities' comments on the existence of the "Regulatory Units", which are autonomous bodies within the State organisational chart with technical autonomy and not subject to any type of mandate or instruction in the scope of their powers, which is that generally recognised in Uruguayan law for general and industry regulatory bodies. The URCDP is similar in organisation to that of the entities created for telecommunications, energy or public information planning purposes.

As for its structure, the LPDP stipulates in Article 31 that the URCDP "Will be managed by a Council made up of three members: the Executive Director of AGESIC and two members appointed by the Executive Power because of their personal backgrounds, professional experience and knowledge in the matter, which guarantee their independent judgement, efficiency, objectivity and impartiality in performing their duties". The Working Party takes note that the reference to the "Executive Power refers to the Presidency of the Republic and that this procedure for the appointment of control body members is the one established in Uruguayan law.

The Executive Council will be assisted by an Advisory Council, which will be made up of five members:

- A person known for his/her record in the promotion and defence of human rights, appointed by the Legislative Power, may not be an active member of parliament.

- A representative of the Judicial Power.

- A representative of the Public Ministry.

- A representative from the academic field.

- A representative from the private sector, who shall be chosen in accordance with the regulations.

Regarding the independence of said authority, the Working Party has found sufficient evidence in Uruguayan legislation, especially since the approval of the DPDP, to conclude that the same is applicable to the URCDP.

Firstly, the LPDP expressly states that the members of the Executive Council "shall not receive orders nor instructions on technical matters"; with the Uruguayan authorities having clarified that this expression must be understood in its broadest possible sense.

Furthermore, Article 29 of the DPDP states that "The administrative actions of the URCDP shall be carried out in line with the principles of impartiality, celerity, efficiency, material truth, informalism, due process, job promotion, good faith, reasoned decisions, and simplicity, which shall serve as an interpretative criterion for resolving any issues that might arise in the processing of any issue".

Meanwhile, regarding the mandate of the Executive Council members, the LPDP establishes a temporary term of office and expressly limits the possibility of discharge, indicating in Article 31 that "Except for the Executive Director of AGESIC, members shall remain in office for four years, with any able to be reappointed. Members shall only cease in their work when they finish their term and their successors are appointed, or when they are discharged by the Executive Power, in cases of incompetence, omission or criminal acts, in line with the guarantees of due process".

The Party is pleased to note that the regulation established in the DPDP strengthens the role of the two members of the Executive Council other than the Executive Director of AGESIC, with the latter's role being reduced and guaranteeing greater independence for the control body.

In this sense, Article 21 of the DPDP stipulates that "The Chairmanship of the URCDP shall alternate annually between the three members of the Executive Council, with the exception of the Executive Director of the Agency for the Development of Electronic Government and the Knowledge-Based Society (AGESIC). During any temporary absence of the URCDP's chairman, the Chairmanship shall be exercised temporarily by a member appointed by the Executive Power", thus removing any possibility of the chairmanship of the body falling to the Executive Director of the AGESIC.

This fact is particularly relevant given that Article 24 a) of the DPDP states that Council resolutions shall be taken by majority, adding that "In the event of a tie, the matter shall be discussed during the following meeting, and if there is no change, the Chairman's vote shall count for two". This prevents the sole disagreement of the Executive Director of AGESIC, whose term of office is subject to a different regime than those of the other Executive Council members, from ever being the basis for any decision taken by the control body.

The Working Party also affirms that the powers of the Chairman of the URCDP include the duty of "Adopting any measures that he/she deems appropriate in emergencies, and giving notice of such during the first Executive Council meeting and abide by any new resolution taken".

Finally, the Working Party accepts that the independence of the control body has been shown in practice as there has been no alteration whatsoever in its activity as a consequence of the change of government that took place in Uruguay in 2009, as can be seen in the information provided to the Working Party by the URCDP, which covers its activities in 2009 and 2010.

Regarding the authority's powers, the Working Party is happy to confirm that these are the same as those established for data protection control authorities in Article 28 of the Directive. Article 34 of the LPDP states that the URCDP will have the following functions and powers:

- To provide assistance and advice to those persons who are in need of assistance and advice to comprehend the scope of the present law and the legal instruments available to protect the rights guaranteed by this law.

- To establish the rules and regulations to be applied in carrying out the activities covered by this law.

- To carry out a census of the databases covered by this law and to keep a permanent register of said databases.

- To monitor the degree to which database controllers comply with regulations governing the integrity, veracity and security of data, being able to carry out any inspections necessary for these purposes.

- To request information from public and private entities, which must provide any background information, documentation, programmes or other aspects required in relation to the processing of the personal data. In such cases, the authority must guarantee the security and confidentiality of the information and elements provided.

- To issue its opinions whenever required to do so by the relevant authorities, including requests related to administrative penalties for infringements of this law, or any regulations or decisions governing personal data processing that are covered by this law.

- To provide advice, whenever necessary, to the Executive Power in drawing up legal bills that relate, wholly or partially, to the protection of personal data.

- To inform any person, free of charge, about the existence of personal databases, their purposes and the identity of the databases controllers.

Furthermore, the LPDP, as shown below, includes specific regulations in relation to investigation, inspection and sanctions, and the DPDP establishes specific regulations for certain procedures to be brought before the URCDP and, particularly, for registering processing and authorising international data transfers.

The Working Party wishes to state that evidence has been provided by the URCDP of performance of these powers in a range of information provided during the analysis of data protection adequacy detailed in this document.

For all these reasons, the Working Party's conclusion on this point is that Uruguay has a supervisory data protection authority with the necessary independence and adequate enforcement competence, in terms similar to those established in Article 28 of the Directive.

Means of implementation and sanctioning.

Article 12 of the LPDP states that "The controller shall be liable for any infringement of the provisions of this law".

One of the functions attributed to the URCDP by Article 34, section e) is "To request information from public and private entities, which must provide the required background information, documentation, programmes or other elements relating to personal data processing. In such cases, the authority should guarantee the security and confidentiality of the information and elements provided.

Article 35 of the LPDP, meanwhile, establishes the possibility of adopting coercive measures in case of infringement of the Law. It states that "The Control Body may impose the following sanctions on the database controllers or processors whenever the provisions of this law are infringed:

a) Warning.
b) Fine amounting to no more than five hundred thousand index units.
c) Suspension of the corresponding database. To this effect, AGESIC is empowered to advise the competent jurisdictional entities to suspend the databases, for a period of up to six working days, for which breach or infringement of the law has been proven.

The coercive functions of the URCDP in this matter are likewise contained in Article 31 of the DPDP, with this control body able to:

- Carry out any inspections that the Executive Council deems pertinent, based on a justified decision.

- Request the relevant court to take appropriate measures if there is a danger of evidence being lost. The request for such measures to be taken shall require a justified decision from the Executive Council.

- Communicate all actions to the database controller or processor so as to confirm them, giving them a period of ten days from the day after notification within which to deal with it. Once this period is over, the actions to be dealt with shall be brought before the Executive Council, which shall have a period of 30 days to announce its decision. The adopted resolution may be contested according to the regulations in force.

In view of what has been stated, the Working Party considers that Uruguayan legislation provides investigation and sanction measures similar to those established for the Member State supervisory authorities in Article 28 of the Directive.

b) To provide support and help to individual data subjects: The data subject must have the possibility to assert his/her rights quickly and efficiently, without excessive costs. To do this, there must be some type of institutional mechanism that allows complaints to be investigated independently.

The Working Party observes that the legislation of Uruguay has introduced various mechanisms designed to fulfil this objective.

Firstly, Article 34 a) of the LPDP states that "The control body must carry out all the necessary actions to comply with the objectives and the other provisions of this law." One of its functions is "To provide assistance and advice to those persons who need this in order to comprehend the scope of this law and the legal instruments at their disposal to protect the rights guaranteed by this law."

An investigation procedure and, where appropriate, sanctioning procedures may be initiated as a result of this activity, given that the procedure may be initiated by the control body itself or at the request of an interested party, as established in the DPDP.

Furthermore, Article 34 h) also includes as a function of the URCDP "To inform any person, free of charge, of the existence of personal databases, their purposes and the identity of the controllers of the databases", regulating their registration procedures and registries.

Together with these duties, Uruguayan legislation provides for measures to be taken to raise awareness about the data protection regulations among both data subjects and those obliged to fulfil these regulations.

For example, this is achieved through transparency in the dissemination of its decisions and opinions. To this effect, the first paragraph of Article 25 of the DPDP states that "The URCDP shall publish any decision taken on its website, after notification. This publication shall be done by applying the relevant criteria established to ensure disassociation of personal data."

The Party considers that the second channel of assistance for parties concerned about the protection of their rights is provided by the "habeas data" action, established in Chapter VII of the LPDP.

Thus, Article 38 of the Law establishes that the data subject may file a habeas data action or write against all controllers of public or private databases, in the following situations:

- When the data subject wishes to see the personal data registered in a database or similar and this request is denied, or is not provided by the database controller, on the occasions and within the time limits established by the law.

- When the data subject asks the controller or processor of the database, to rectify, update, eliminate, include or delete data, and the controller does not do as requested, or does not provide sufficient reasons for the failure to do so within the time limits established by law.

This is a legal action that is processed quickly, and which may be filed by the data subject or his/her legal representatives and, in the case of deceased persons, by their universal successors. It is governed by procedural regulations with the specialities established in the LPDP.

According to Article 43 of the LPDP "A judgement based on the writ of habeas data should include:

- Clear identification of the authority or person against whom it is brought and against whose action, deed or omission the habeas data is issued.

- A precise order indicating what should or should not be done and, if applicable, the term period during which said decision shall remain in force.

- The time period for complying with the decision, which shall be set by the court according to the circumstances of each case, and will not be longer than 15 consecutive and uninterrupted calendar days, counted as of the notification date.

In view of the aforementioned information and as already indicated, the Party considers that Uruguayan legislation offers sufficient mechanisms to provide assistance and support to interested parties.

> **c**) **To provide appropriate redress to those affected when regulations are not observed:** This is a key element that must be included in a system that provides the possibility of obtaining a legal or arbitration decision and, where applicable, compensation and sanctions.

Article 12 of the LPDP states that "The controller shall be liable for any infringement of the provisions of this law".

The Working Party notes that, by virtue of the provisions of this article and the general regulations of Uruguayan civil law, and in particular of its Civil Code, any interested party who has suffered damages as a consequence of their personal data being processed may request the relevant redress. Said redress may include the material damages suffered as well as moral damages.

Therefore, the Party considers that this guarantee is properly established in Uruguayan law.

4. RESULT OF THE ASSESSMENT

In conclusion, pursuant to all the above, the Working Party considers that **the Eastern Republic of Uruguay ensures an adequate level of protection** within the meaning of Article 25(6) of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

The Working Party also highlights the fact that, as part of any decision taken by the Commission, it will closely follow the evolution of data protection in Uruguay and the way in which the Data Protection Authority ("URCDP") applies the principles of data protection referred to in document WP12 and in this document.

In Brussels, on 12 October 2010

For the Working Party,
The Chairman
Jakob KOHNSTAMM