



SELF-REGULATION AND PERSONAL DATA PROTECTION

(DOCUMENT PREPARED BY THE WORKING GROUP MEETING AT SANTA CRUZ DE LA SIERRA –BOLIVIA- ON 3-5 MAY 2006)

SUMMARY: I. ANTECEDENTS; II. SELF-REGULATION AND PROTECTION OF PERSONAL DATA: 1. Statutory references; 2. Scope, effectiveness and content of the self-regulation instruments; III. RECOMMENDATIONS

I. ANTECEDENTS

The Latin American Data Protection Network (hereinafter “*RedIPD*”), was founded in June 2003, in La Antigua, Guatemala, in order to encourage initiatives of exchanging experience between Latin American countries and reinforcement of mutual, continual collaboration, with a view to promote, mainly, statutory frameworks and to encourage wider implementation of a personal data protection culture.

In the Declaration of La Antigua, the RedIPD saw the “*need to foster measures that guarantee a high level of data protection, and they perceive the suitability of having national legislative frameworks*” that provide adequate protection for all the Latin American countries.

The Declaration by the 13th Latin American Summit Meeting of Heads of State and Government, signed on 15 November 2003 in Santa Cruz de la Sierra, Bolivia, specifically recognised that “*the protection of personal data is a*



fundamental right of all persons” and it emphasised “the importance of Ibero-American regulatory initiatives for protecting the privacy of citizens contained in the La Antigua Declaration creating the Ibero-American Data-Protection Network”.

Subsequently, the final declaration issued on the occasion of the 28th World Data Protection Conference, held in Montreux, Switzerland, in September 2005, also emphasised the importance of the work carried out by the RedIPD.

In the Declaration of Cartagena, issued in May 2004, the RedIPD stated that it is necessary *“to promote and encourage self-regulatory initiatives that complement and facilitate application of the regulatory framework”* on data protection. The nature of such instruments is that of *“codes of standards or good practice, and they are a fine instrument for boosting the adequate processing of personal data, because the complement or implement already existing regulatory frameworks”*. There, it also recommended both the need to publicise these, for them to be known, as well as to submit such initiatives to scrutiny by the controlling authorities. *“Doing so can reveal how well such codes adhere to the rules of personal data protection, thus assigning them an added value of guarantee, quality and trust, without detracting from the obligations established in current legislation on data protection.”*

In the Mexico Declaration of November 2005, the RedIPD created the set of *“Self-regulatory Instruments”* to analyse the validity and effectiveness of the codes of conduct or similar instruments, bearing in mind that:

- It is important that the general and sectorial rules handed down by the State be added to the initiatives of the actual operators, in order that personal data protection be performed through self-regulation mechanisms.



- Self-regulation alone is not enough to achieve an adequate legal protection system to protect a fundamental right, because its protection would be left to the entities affected, excluding intervention by the public powers.
- The above *“does not mean that self-regulatory initiatives are not useful in supplementing a legislative framework previously defined by the State”* because *“self-regulatory instruments may afford added value to personal data protection, whether corporative initiatives are undertaken to provide greater quality in the processing of customers' personal data, given the insufficient nature of the regulations approved by the State, or endeavour to offer further guarantees in addition to those envisaged in such legislation. Such initiatives may enable adaptation of the legislation to the specific characteristics of data processing in a certain sector, allowing the creation of standards specifically adapted to the needs of that sector, and thus facilitating their observance.”*

Due to the preceding mandate, the Working Group, met at Santa Cruz de la Sierra, Bolivia, on 3-5 May 2006 prepared and approved this document.



II. SELF-REGULATION AND PROTECTION OF PERSONAL DATA.

1. Statutory references.

- A. There are international documents that promote the use of self-regulatory instruments within the field of data protection. For illustrative, but not exhaustive purposes, we cite the following: (1) Article 27 of Directive 95/46/EC¹ by the European Parliament and Council, establishes that the Member States and Commission encourage professional associations and other organisations representing data controllers to draw up “*codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors*”. These codes must be submitted to review by the local authorities so they may be compatible with the national provisions and; to the extent possible, one may take into account suggestions by persons eventually affected by processing of their personal data; (2) the Joint Declaration EU-USA on electronic commerce of 5 December 1997 establishes the need to “*ensure effective protection of the right to privacy with regard to automatic processing of personal data on global information networks*” and emphasises the importance of self-regulation due to an agreement between the industry and other private sector institutions. Due to this, they agreed “*to actively support development, preferentially at global level, of codes of conduct based on self-regulation and technologies that allow increased consumer confidence in e-commerce, involving all partners on the market, including those who represent the consumers’ interests*”; and (3) The OECD Council, on the

¹ Concerning the protection of individuals with regard to processing of personal data and free flow of such data (24 October 1995)



other hand, stated in its Document on Guidance for Consumer Protection in the context of Electronic Commerce (1999) that such commerce should be conducted according to principles of privacy that propose appropriate, effective protection of that consumers' right. To that end, it suggested that States, among others, review, amend and encourage “*self-regulatory practices*” to “*make them compatible and applicable to e-commerce*”. There, it also emphasised the importance of participation by “*representatives of the consumers in development of self-regulatory mechanisms containing specific and substantiate rules applicable to complaint management and dispute solving procedures*”.

B. In that same sense, there are general and sectorial national laws in the Latin American countries that not only promote creation and implementation of self-regulatory instruments, but also show the importance of coexistence and the complementary nature of such regulatory models. As an example, we emphasise the following in alphabetical order:

COUNTRY	LAWS
Argentina	<p>Article 30 of Act 25326 of 2000:</p> <p><i>“Codes of conduct</i></p> <p><i>1.- The associations or entities representing data controllers or users of privately-owned data banks may create professional practice codes of conduct, establishing the rules for the processing of personal data tending to assure and improve the operational conditions of information systems on the basis of the principles established by this Act.</i></p> <p><i>2.- Such codes shall be registered with the register kept by the controlling body, who may deny registration whenever it considers that the said codes do not conform with</i></p>



	<p><i>the legal and regulatory provisions governing the matter.”</i></p> <p>* Letter f of number 5 of Article 29 of Decree 1558 of 2001</p> <p><i>“5. The duties of the NATIONAL PERSONAL DATA PROTECTION DIRECTORATE (DNPDP), in addition to those that arise from Act No. 25.326: (...) . f) to endorse the codes of conduct that arise with regard to the terms of article 30 of Act No. 25.326, following finding by the Consultation Council, taking into account their adaptation to the regulatory principles on processing of personal data, the representativity that is exercised by the association and body that prepares the code and its executive efficiency with regard to the operators in the sector by means of the provision of penalties or adequate mechanisms.</i></p> <p>* Article 30 of Decree 1558 of 2001:</p> <p><i>The DNPDP must promote “preparation of codes of conduct aimed at contributing, according to the specific nature of each sector, the correct application of the national provisions adopted by Act No. 25.326 and this regulation.”</i></p>
Spain	<p>* Article 32 of Organic Act 15/1999 of 13 December.</p> <p><i>“Standard codes of conduct</i></p> <p><i>1. By means of sectorial agreements, administrative agreements or company decisions, publicly and privately-owned controllers and the organisations to which they belong may draw up standard codes of conduct laying down the organisation conditions. The operating rules, the applicable procedures, the safety standards for the environment, programs and equipment, the obligations of those involved in the processing and use of personal information, as well as the guarantees, within their remit, for exercising the rights of the individual in full compliance with the principles and provisions of this Law and its implementing rules.</i></p> <p><i>2. These codes may or may not contain detailed operational rules for each particular system and technical standards for their application. If these codes are not incorporated directly into the code, the instructions or orders for drawing them up must comply with the principles laid down in the code.</i></p> <p><i>3. The codes must be in the form of codes of conduct or of good professional practice,</i></p>



	<p><i>and must be deposited or entered in the General Data Protection Register and, where appropriate, in the registers set up for this purpose by the Autonomous Communities, in accordance with Article 41. The General Data Protection Register may refuse entry when it considers that the code does not comply with the legal and regulatory provisions on the subject. In such a case, the Director of the Data Protection Agency must require the applicants to make the necessary changes.</i></p> <p>*Article 9 of Royal Decree 1332/94 of 20 June.</p> <p><i>“Inscription and advertising of standard codes.</i></p> <p><i>The standard codes will be deposited, for their inscription, at the Data Protection General Register.</i></p> <p><i>The Director of the Data Protection Agency may refuse the registration if the standard code does not comply with the provisions of Organic Act 5/1992 and this Royal Decree, notwithstanding requiring the applicants to correct the defects.</i></p> <p><i>Private individuals may obtain copies of the standard codes deposited and registered at the Data Protection General Register.</i></p> <p><i>In the event of breach of the rules contained in the standard codes, the terms provided to that end in the resolutions or decisions that formulated them will apply”.</i></p>
Peru	<p>* Complementary final provision two of the Regulations of Act 28493 that regulates spam.</p> <p><i>“The Ministry of Transport and Communications promotes the use of self-regulatory and technical mechanisms by the industry. Internet service providers must include codes of conduct in their use policies concerning correct use of electronic mail,(...)”</i></p>
Portugal	<p>* Article 32 of Law 67/98 of 26 October.</p> <p><i>“Codes of conduct.</i></p> <p><i>1 – The CNPD shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the provisions in this Act, taking account of the specific features of the various sectors.</i></p> <p><i>2 – Trade associations and other bodies representing other categories of controllers which have drawn up draft codes of conduct shall be able to submit them to the opinion of the CNPD.</i></p>



	<p>3 – <i>The CNPD may declare whether the drafts are in accordance with the laws and regulations in force in the area of personal data protection.</i></p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------

2. Scope, effectiveness and content of the self-regulation instruments.

A. In the context of personal data protection, self-regulation refers to the rules adopted by the bodies to define their policies and commitments with regard to personal data processing. In that sense, for example, the European Commission has defined it as the set of rules *“applying to a plurality of data controllers from the same profession or industry sector, the content of which has been determined primarily by members of the industry or profession concerned.”*². This concept presupposes that various members process third party personal data. However, one must bear in mind that, in some countries, that task is performed by companies that practically have the monopoly over gathering, storage, flow and use of the data of citizens or, in other cases, processing is performed by a few competing companies among which it is not easy to establish a consensus on the matter. Due to the foregoing, self-regulation also includes scenarios in which there is not necessarily a plurality of data controllers.

B. The focus and degree of development of the policies and tools for protection of personal data in Latin American countries is

² European Commission. Working Party on the Protection of Individuals with regard to the Processing of Personal Data. Working Document DG XV D/5057/97: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?. Adopted in 14 January 1998.



heterogeneous. We all hope to have the legal, administrative and financial instruments to guarantee an adequate level of protection of personal information. However, reasons of a different nature show that the scenario of mechanisms to that end is different, as we encounter other countries that have an integral sectorial regulation linked to the existence of autonomous, independent control bodies (although to a different extent) and even countries that, for the moment, only have sectorial regulations, without control by a data protection authority. These differences will have an effect on greater or lesser contribution by self-regulation instruments to promote or strengthen personal data protection.

C. It is important that data controllers create self-regulation mechanisms for the following reasons: (1) It represents a positive manifestation of the social responsibility of the companies to guarantee fundamental rights, creating mechanisms that grant additional guarantees or benefits in relation to the terms of the statutory frameworks; (2) the due implementation of self-regulation instruments facilitates fulfilment of the principles of data protection and raises quality standards in this field; (3) correct processing of personal data generates personal confidence and facilitates information exchange; (4) there is proof of the trend in people preferring to do business or carry out activities with companies that guarantee high levels of personal data protection; (5) the existence and application of codes of conduct may represent a competitive advantage for companies to the extent that this is a factor people take into account when performing activities with third parties; (6) companies may position and increase their good name and confidence among customers and society at large by showing their interest and commitment to personal data protection.



D. Self-regulation does not substitute the indispensable management and responsibility of the States, to recognise and effectively guarantee protection of the fundamental right to personal data protection.

E. Notwithstanding the foregoing, self-regulation provides a complementary tool to the regulatory framework that not only contributes to consolidate a protection culture for such a fundamental right, but also encourages, strengthens and consolidates the correct processing of the information on persons, to the extent that said instruments are effectively applied and guidelines consecrated to show a true additional value of these with regard to the legislation.

F. Self-regulation may not be understood as the sole voluntary implementation of codes of conduct that repeat what is established in the laws. Real protection of personal data requires those instruments to have an effective application. Self-regulation initiatives will not take effect if the companies do not fulfil those rules and if failure to abide by them has no consequence.

Thus, self-regulation will not only provide real benefit for persons to the extent that it is well conceived and applied, having mechanisms to guarantee its fulfilment, so it does not constitute mere symbolic declarations of good intentions.

G. By virtue of the foregoing, it is indispensable for the self-regulation instruments to be accompanied by tools that make them effective. Among these mechanisms, the following are suggested: (1) Establishing agile, free, effective means so that, in the event of breach



of the code, the subject may not only demand respect for his rights and liberties, but rather become an “auditor” of the management by the controller of his personal data. (2) To consecrate internal and external control mechanisms for verification of the fulfilment of the codes, and (3) To provide penalties for breach of the codes.

H. Self-regulation measures must be evaluated from the concomitant perspectives: objective and functional. The first aims to determine whether the content of these consecrates an added value and whether it is in compliance with local laws or, if these do not exist, the international principles on data protection that have been established in the documents issued, among others, the UNO, the European Union and the OECD. The second, on the other hand, seeks to establish the level of practical effectiveness of those regulations. An analysis of the above factors will allow one to determine the true degree of contribution by the self-regulation instruments to personal data protection.

I. Self-regulation instruments must be clearly and accessibly drafted to establish the data protection to be applied to personal data processing by the signatory entities, including the specific rules and standards that guarantee fulfilment of the principle of purpose and quality of the data, the right to information in data gathering, the existence of consent by the data subjects, adoption of security measures for the data and, if appropriate, the applicable conditions in the communication or international transfer of data to third parties, in order to harmonize data processing performed by the signatories. They must also record the procedures to be used to allow the data subjects to exercise the rights of access, correction, opposition and cancellation of data.



Moreover, self-regulation instruments may be used to foresee training actions in matters of data protection, aimed at those performing data processing, especially with regard to their relation with the data subjects. They may also include a quality seal to identify their members.

Those responsible for self-regulation instruments must publicise their existence, preferably through computer or telematic means, detailing and publicising the identity of the member entities.

On the other hand, it is considered appropriate to provide formulas for periodic evaluation of the self-regulation instruments, measuring the degree of satisfaction of the data subjects and, if appropriate, updating the content to adapt it to the general or sectorial regulations on data protection that exist at each moment.



III. RECOMMENDATIONS

1. Inclusion, in the legal texts on data protection, specific provisions aimed at using self-regulation mechanisms that: (a) Represent an added value in their content as provided in the laws, and (b) That contain or are accompanied by mechanisms that allow their level of efficiency to be measured with regard to fulfilment and the degree of protection of personal data.
2. Inviting the States and data controllers to promote adoption and application of self-regulation mechanisms in the different sectors.
3. Conception of self-regulation as a non substitutory, nor sufficient mechanism alone, to guarantee personal data protection and as a tool to complement the legal framework to encourage the culture of personal data protection.
4. Consecration of effective measures in the event of breach of the instruments of self-regulation.
5. Promotion of publicity mechanisms for the self-regulation instruments, with special consideration for the existence of public registries.