



VIABILITY OF THE ESTABLISHMENT OF SUPERVISORY AUTHORITIES IN LATIN AMERICA

TABLE OF CONTENTS

- I. INTRODUCTION**
- II. OVERVIEW OF THE SITUATION**
- III. MODELS FOR DATA PROTECTION SUPERVISORY AUTHORITIES**
 - 1. EUROPEAN MODEL**
 - 2. SCENARIO IN LATIN AMERICA**
 - 3. CHOICE OF A MODEL**
- IV. CONCLUSIONS**



VIABILITY OF THE ESTABLISHMENT OF SUPERVISORY AUTHORITIES IN LATIN AMERICA

I. INTRODUCTION

The working group on the viability of the establishment of supervisory authorities in Latin America (Viability Group) within the *Red Iberoamericana de Protección de Datos* (Latin American Data Protection Network) was constituted in the *Declaration of Cartagena de Indias* on 28th May 2004.

The consolidation of the fundamental right to data protection encompasses the need for an essential complement: the existence of rapid, immediate and effective guarantee mechanisms to defend the public against violations of this right by government or individuals.

Such defence may take on many show and its structure in each country depends on many variables, including legal, economic and social conditions, amongst others.

On the basis of the advisability and need for control authorities, this Group has set out a series of recommendations addressed at the countries in our Region describing a model supervisory authority framework with extensive controlling powers, as well as other alternative models that can undertake the same tasks with very different structures, powers and organisation, and are sufficiently flexible to adapt to each country in function of its particular legal and social scenario.

In this respect, we are aware of the possible economic and social difficulties that may impede the creation of such an authority and we propose certain ideas that may facilitate the establishment of data protection bodies that will be able to guarantee the right to data protection in our region.

The choice of one or another model is a decision that must be taken nationally, and a number of factors must be taken into account to ensure the success of the envisaged supervisory body.

II. OVERVIEW OF THE SITUATION

The introduction of the so-called “new technologies” into Latin American society and the development of the Information Society in this area have fuelled new economic and social drive. Personal data processing is closely



VIABILITY OF THE ESTABLISHMENT OF SUPERVISORY AUTHORITIES IN LATIN AMERICA

linked to the advance of the new information technologies, implying a considerable leap in cross-border data flows, through companies operating in various countries or through exchanges of data in cooperation amongst governments. Thus, personal data processing has now become unavoidable in many sectors of activity.

The adoption of measures that guarantee a suitable and uniform degree of data protection throughout the entire region is clearly a priority in an endeavour to remove barriers and promote continual improvement in the living conditions of all peoples, to boost the operation of a Latin American market and the free circulation of goods, persons, services and capital, and to ensure protection of the fundamental rights of all.

There are significant differences in the degree of data protection between the Latin American and the European countries, and these differences represent an obvious obstacle to business activities that require continual flows of data.

The provisions of the European Directive on the international flow of data establish that the country receiving such data must guarantee a suitable degree of protection. According to the European Council, a Supervisory Authority is an essential factor in such personal data protection.

To avoid these differences, bring the various national situations into line and pave the way for a more secure environment for the public, mechanisms must be found to ensure an equivalent degree of data protection in the area, through the approval of national legislation and the creation of supervisory authorities to oversee observance of the right to personal data protection.



VIABILITY OF THE ESTABLISHMENT OF SUPERVISORY AUTHORITIES IN LATIN AMERICA

III. MODELS FOR DATA PROTECTION SUPERVISORY AUTHORITIES

The need for a supervisory authority was recognised by the United Nations, in principle eight of the *Guidelines for the Regulation of Computerised Personal Data Files*, adopted by resolution 45/95 of the General Assembly on 14th December 1990. This principle establishes that the law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the data protection principles. This authority shall offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence.

A final Declaration on *"The protection of personal data and privacy in a globalised world: a universal right respecting diversities"* was recently ratified at the 28th International Conference on Privacy and Data Protection held in Montreux, Switzerland from 13th to 15th September 2005. This Declaration makes express reference to the principle of independent supervision as one of the foundations of the right to data protection and concludes by urging all governments to set up the legal privacy and data protection mechanisms to comply with the aforesaid principle of independent supervision.

1. EUROPEAN MODEL

The terms of Convention 108 of the European Council of 1981, *for the Protection of Individuals with regard to Automatic Processing of Personal Data* must be taken into consideration in defining the fundamental components of a personal data supervisory authority, while its Additional Protocol clearly establishes the need for independent authorities in each country charged with overseeing observance of data protection regulations and establishing their essential characteristics. This same structure, with only minimal changes, was established in the European Data Protection Directive of 1995 (Directive 95/46/EC).

The European Union Charter of Fundamental Rights, adopted in Nice on 7th December 2000, ratifies the principle that respect for data protection regulations shall be subject to the supervision of an independent authority.



VIABILITY OF THE ESTABLISHMENT OF SUPERVISORY AUTHORITIES IN LATIN AMERICA

Directive 95/46/EC establishes that each Member State shall provide one or more public authorities that are responsible for monitoring the application within its territory of the data protection provisions. These authorities shall act with complete independence in exercising the functions entrusted to them, be endowed with investigative powers (to collect all the information necessary for the performance of their supervisory duties); effective powers of intervention (delivering opinions before processing operations are carried out); and the power to engage in legal proceedings where the national provisions have been violated.

The Authorities shall hear claims lodged by the affected parties related to the protection of their rights and freedoms as regards personal data protection.

With respect to the public nature and transparency of their activities, the Directive establishes that such Authorities shall present reports on their activities at regular intervals – in practise, annually.

Moreover, the Directive endorses and calls for cooperation amongst the different Authorities to the extent necessary for the performance of their duties and, in particular, through the exchange of all useful information.

To ensure confidentiality, the Directive provides that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

The Spanish Data Protection Agency (AEPD) was set up according to the model described above, and its legal framework is established in the Data Protection Act of 1999 (LOPD).

The AEPD has the following characteristics:

- It is an independent Authority.
- It is headed by a Chairman who is elected from amongst the members of a Consultative Council for a 4-year term of office.
- Its decisions can only be revoked by the *Audiencia Nacional* (the National Court of Spain).



VIABILITY OF THE ESTABLISHMENT OF SUPERVISORY AUTHORITIES IN LATIN AMERICA

- With respect to transparency in its activities, it is required to submit an Annual Report to the Spanish Parliament, which is also published *on-line*. Likewise, the Agency publishes its legal reports and sanction rulings, all of which may serve as a guide for the public and comprise a consolidated code of conduct. The foregoing is undertaken fully respecting the guarantee of privacy for the parties involved (all personal data cited in the rulings is dissociated).
- The AEPD is endowed with supervisory powers (investigations, sanctions, etc.).
- It guarantees the public nature of existing personal data processing through the General Data Protection Registry.
- It assists citizens in the protection of their rights and processes claims lodged regarding violations of the LOPD.
- Its financing runs on an annual budget chosen by the General State Budget, supplemented by other auto-financing systems.

Together with the legal framework established in the LOPD, since 2003 the Spanish Data Protection Agency has also been charged with new responsibilities related to privacy in telecommunications, attributed by General Telecommunications Act 32/2003 and Act 34/2002 on Information Society Services. These new duties primarily refer to vigilance with respect to unsolicited bulk e-mail ("*spam*").

The Portuguese National Data Protection Commission, created in Act 67/98 on Personal Data Protection, also follows the European Model.

Likewise, and although it is not a Member of the European Union, the Andorra Data Protection Agency was established in application of Act 15/2003, on the protection of personal data.



VIABILITY OF THE ESTABLISHMENT OF SUPERVISORY AUTHORITIES IN LATIN AMERICA

2. SCENARIO IN LATIN AMERICA

The majority of the Constitutions of the Latin American countries guarantee the right to privacy and, explicitly or implicitly, the protection of personal data. However, these countries do not have specific laws on this matter, with the exception of certain cases.

This means that many Latin American countries do not have authorities whose duties substantially and specifically encompass the supervision of personal data protection.

An exception to this scenario is Argentina, which has established the *Dirección Nacional de Protección de Datos Personales* (National Directorate of Personal Data Protection), as a decentralised body under the Ministry of Justice and Human Rights, with operational autonomy and headed up by a Director appointed by the Government after the relevant official examination for a period of four years (article 29 of Act 25.326).

The National Directorate of Personal Data Protection, created by legal decree 1558/2001, is endowed with investigative and intervention powers, as well as being charged with assistance and advisory duties. It is empowered to adopt rules and regulations to implement the law, and operates a Registry of public and private databases. In addition, this supervisory body can also lodge complaints in criminal actions, supervises observance of the requirements and guarantees established to register data banks in the Registry and is empowered to impose sanctions.

For further information on legislation, authorities and projects, please consult the Comparative Table of National Development drawn up by the *Red Iberoamericana de Protección de Datos*¹.

3. THE CHOICE OF MODEL

In addition to the aforementioned advantages afforded by the existence of a supervisory authority in ensuring that the personal data of individuals will be

¹ Website www.agpd.es, section entitled “Red Iberoamericana de Protección de Datos”



VIABILITY OF THE ESTABLISHMENT OF SUPERVISORY AUTHORITIES IN LATIN AMERICA

used legally and legitimately, and that the public will have the effective tools and resources to exercise their rights, the creation of such authorities also fosters an atmosphere of greater trust in the parties involved in commercial transactions, which thereby facilitates the international flow of data that is essential in global economic relations today.

In this respect, it is important to remember that one of the requirements set out by the European Union for a third party country to be considered to have a suitable degree of protection is the existence of an independent supervisory authority endowed with genuine supervisory powers.

It is also necessary to consider that the eventual adoption of a model framework may face restrictions of an economic or regulatory nature. In this case, alternative models that pursue the goal of personal data protection and mitigate the economic and institutional expense of their implementation through a more efficient use of resources must be sought.

IV. CONCLUSIONS

The Viability Group:

- Ratifies the opinion that Supervisory Authorities play a fundamental role in effective personal data protection.
- Proposes the so-called European Supervisory Authority model described above as the model of reference.

Nonetheless, in accordance with the current scenarios in each country, projects for the creation of these autonomous, independent authorities may be preceded by solutions that provide the supplementary, non-exclusive alternatives set out below.

Alternative 1: Use the already existing administrative, constitutional and legal structures.

- The primary duties of the Authority, as described in the European model, may be undertaken by already existing administrative bodies – not



VIABILITY OF THE ESTABLISHMENT OF SUPERVISORY AUTHORITIES IN LATIN AMERICA

specifically engaged in data protection – provided a mechanism is put in place to guarantee their independence.

- Such duties may be undertaken by constitutional bodies entrusted with the protection of the fundamental rights of its citizens (ombudsmen, public ministries, etc).
- The creation of speedy, free, legal mechanisms for the defence of data protection and habeas data.

Alternative 2: Create supplementary protection bodies and mechanisms in the public sphere.

- The implementation of e-government policies and modernisation of the State must take into account the implications of the same on data protection. The possibility of creating supervisors or bodies in charge of data protection in this sphere may be envisaged.
- Reorganisation of the existing administrative bodies to create new units that do not imply greater expense, but rather rationalise material assets and human resources to guarantee a fundamental right that was ratified in the *Declaration of Santa Cruz de la Sierra* and must be implemented through concrete actions.

Alternative 3: Promote greater cooperation from the private sector.

- To foster the creation of experts, or “data protection officials” as an efficient way to reach a greater degree of observance.
- To encourage self-regulation by the interested parties themselves, such as, for example, through codes of conduct.

Huixquilucan (Mexico State), 4th November 2005