CARTAGENA DE INDIAS DECLARATION

made on the occasion of the

THIRD IBERO-AMERICAN MEETING ON DATA PROTECTION

25-28 May 2004

The participants in the Third Ibero-American Meeting on Data Protection held in Cartagena de Indias, Colombia, on the 25th to 28th May 2004 to reflect upon *'Personal data protection as a guarantee of service quality: New challenges and opportunities for the financial, commercial and telecommunications sectors in Ibero-America',* wish to make public the findings of the Meeting.

They voice their satisfaction with the progress that has been made since the Meeting in La Antigua, Guatemala, in June 2003, which progress has taken the form of a number of regulatory drafts in the field of personal-data protection and the consolidation of permanent channels for cooperating and sharing experiences, documents and opinions on matters of data protection.

The participants are particularly congratulated that the Heads of State and Heads of Government of the Ibero-American countries meeting at their Thirteenth Summit Meeting in Santa Cruz de la Sierra, Bolivia, on the 14th and 15th November 2003 expressly acknowledged the importance of the fundamental right to data protection, whereas they stated as follows in point 45 of the summit's final declaration:

'Likewise we are aware that the protection of personal data is a fundamental right of all persons, and we highlight 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, open to all the countries of our Community'.

The Santa Cruz de la Sierra Declaration recognises the work of the Ibero-American Data-Protection Network and therefore spurs us to redouble our efforts on behalf of the fundamental right to data protection. The participants therefore take up the commitment to continue along the path they have begun, where they shall seek to achieve the broadest possible introduction of the culture of data protection, based on national regulatory frameworks that, as

called for in the La Antigua Declaration, guarantee adequate protection of this fundamental right in all Ibero-American countries.

Thus, the participants consider it indispensable to bring the Network's opinion to the attention of the Ibero-American Community, in hopes that in this fashion an objective, impartial point of reference can be settled upon for use in the effective implementation of the fundamental right to the protection of personal data, a fundamental right that the participants are convinced wields a decisive influence on the social and economic development of Ibero-American countries.

As a consequence, bearing in mind the speeches and papers presented and the result of the enriching discussions held, the participants now make public the following

FINDINGS

I. DATA PROTECTION AND THE PERSPECTIVE OF THE FINANCIAL SECTOR

Fair, legal, transparent, ethical processing[1] of personal data is a guarantee all persons hold, and it must be respected in the pursuit of objectives such as preserving the stability of the financial system and facilitating access to credit. The acquisition and use of personal information to mitigate and administrate the risks implied in extending credit must be accompanied by respect for the rights of all persons in the processing of personal data. Effective protection of financial data helps make people more willing to support the flow of information about themselves. In striving after these objectives, the activity of public credit bureaus such as *centrales de riesgo públicas* and private credit bureaus such as *centrales de información crediticia*[2] (CIC) is important. The latter type of credit bureau makes it easier for its users to gange credit risk.

In addition to the incorporation of the essential principles of data protection recognised in national and international instruments, the regulation of personal-data protection should envisage guidelines that recognise the unique features inherent in financial data.

[1]Within this document, this expression shall be understood to refer to any operation or set of operations performed by computerised or other procedures and applied to personal data, inter alia, collection, recording, organisation, storage, creation or amendment, extraction, consultation, use, communication, dissemination or any other operation facilitating access to data or collation or interconnection of data, data blocking, data elimination or data destruction.

[2]This expression includes credit bureaus, *centrales de riesgo, protectoras de crédito* and generally any private database or enterprise that engages in the processing of personal data in order to evaluate risk.

Legislative developments must enable information to flow to financial intermediaries so they can evaluate their business risks, and it must guarantee the fundamental right to the protection of personal data, such that there is a balance between the two goals.

Collecting and circulating financial data about people has become a valuable tool for a more solid, modern, competitive financial system.

Thus, *centrales de riesgo públicas* (CRPs), because they guarantee the stability of the financial system, must have the ability to process the necessary data to comply with that mission.

CICs help deal with the information asymmetries in credit markets, foster a culture of payment and generally contribute to the development of credit activity on healthy bases.

Financial service providers and consumers alike reap the benefits when they operate in a market with better-quality information about people. The information that CICs transmit to third parties must be high-quality, reliable information. Therefore, it must be truthful, accurate, full and updated.

Despite progress and national and international efforts in these directions, situations continue to appear in which, for a variety of reasons and circumstances, financial data about people is improperly processed. That is why all the players involved in the processing of this type of information (inter alia, CRPs and CICs, plus their sources of information) must boost and strengthen measures to guarantee an adequate level of protection for information on financial-sector users at all times. This effort should be accompanied by speedy, effective customer service with a view to respecting customers' rights to access, update and rectify their personal information; these rights, in addition to constituting a guarantee for citizens, enable the quality of the information in databases to be enhanced. Additionally, the fostering of an organisational culture of data protection inside CRPs and CICs and their sources of information will also help reach the aforementioned goal.

The steps discussed above not only will engender more citizen trust in how credit data are processed, but also will constitute an imperative for respecting legal and ethical obligations in the processing of personal data.

II. THE FIGHT AGAINST SPAM

The growing development of information highways has brought into day-to-day life instruments that facilitate electronic connections between the different

realms in which people go about their daily business. Electronic communications are an immediate, fast and economical way for the users of the different public telecommunications networks to contact one another.

In the shadow of this highly useful instrument, a practice has developed whereby unwanted electronic communications or data messages popularly known as spam are sent to unconsenting recipients. Although doctrine does not speak with a single voice when addressing the concept of spam, 'spam' is normally understood to refer to the process of sending unsolicited, undesired information. Spam has grown exponentially in recent years, due fundamentally to the low cost of services, the ease with which e-mail addresses can be obtained and the difficulty of identifying spammers, who can usually find some technological means of concealing their identity. Spam has therefore become a global problem that affects practically all sectors of production and the economy, in addition to property entitled to legal protection.

The presence of spam in the daily life of the users of public telecommunications networks has triggered a strong backlash against indiscriminate spamming, due to spam's negative impact on the protection of other legal property and user rights that deserve protection. Because spam illegitimately intrudes into users' privacy, because spam does economic harm to citizens and enterprises, because spammers send contents that are in many cases misleading and fraudulent, society is demanding measures to fight against this type of practice.

Technological measures must be taken to control and filter out spam. Such measures are necessary, although by themselves they will not suffice to counteract the growth of spam. Legislative measures should be taken that specifically discipline the fight against spam, guaranteeing the rights of users and regulating to the necessary extent the activities of the different agents involved in this activity. International cooperation on this subject will enable a uniform framework to be created; such a framework is vital for combating spam, for the phenomenon is transnational in scope. It is necessary also to create a favourable atmosphere for and encourage sector-specific self-regulation initiatives to complement and facilitate the application of the regulatory framework on spam.

Lastly, it is vital for measures to be taken to boost users' awareness of the harm that spam does to them. This way, the agents that make the propagation of spam possible will find their activities hampered by greater user education, which will help actively to prevent this problem, which features involves multiple interdependent factors.

III. INTERNATIONAL DATA TRANSFERS: EUROPEAN AND IBERO-AMERICAN PERSPECTIVES

International transfers of personal data must be placed under a system of guarantees to prevent the principles governing the fundamental right to data protection from being violated simply by shifting personal data to another country.

The European Union Data Protection Directive has enshrined this principle and given the European Commission the power to decide when a country that has established data-protection legislation that meets European standards and created an independent supervisory authority is a secure destination for personal data from EU Member States. This recognition is equivalent to the full liberalisation of exchanges of personal data between the European Union and the country in question, which greatly favours commercial exchanges and, more specifically, the development of electronic commerce and Information Society services.

In 2000 the Argentine Republic enacted Personal Data Protection Act Number 25,326. This act, together with Decree 1,558 of 2001 regulating the act, vested Argentine law with a solid data-protection regime that included all the essential principles that ought to govern the licit, legitimate processing of personal data: proportionality, purpose, information for the data subject, quality, special protection for certain categories of data, confidentiality, security and data subjects' rights of access, rectification and elimination. Also established was an independent supervisory authority, the National Directorate for the Protection of Personal Data, through which data subjects can exercise their rights quickly and effectively. The guarantees furnished by this legislative and supervisory framework were recognised by the European Commission, which considered, in Decision 2003/490/EC of 30 June 2003, that Argentine legislation afforded an adequate level of data protection.

When there is no such acknowledgement, it is possible, among other options, to use the standard contract clauses approved by the European Commission. These clauses provide one way of establishing the necessary guarantees to make up for a lack of adequate legislation in the country of destination, because the clauses grant the subjects whose data are transferred the possibility of demanding enforcement of the contract clauses pertaining to them and reparation in the event of damages due to breach of contract.

Therefore, the participants in the Third Ibero-American Meeting on Data Protection earnestly hope that the Ibero-American countries will enact data-protection regulations and establish independent supervisory mechanisms that promote an effective introduction of the fundamental right to the protection of

personal data and at the same time facilitate the free flow of personal data between countries.

IV. THE TELECOMMUNICATIONS SECTOR AND THE INTERNET IN ATTACKS ON PRIVACY

With the development of the information society, new electronic communications products and services have appeared that have done much to improve users' ability to access information.

For example, added-value services have arisen in recent years that facilitate economic activity and lead to a better quality of life for citizens.

At the same time, the exponential growth of the Internet over the last ten years is providing access to a huge quantity of information, which makes available a greater wealth of knowledge about a vast range of subjects and also enables each user to communicate with an increasing number of other people at opposite ends of the earth.

Providing all these information-society services necessarily entails processing personal data, which users must sometimes furnish in order to gain access to the information or services they require. Nevertheless, the processing of personal data can pose risks to users' privacy and their fundamental right to personal-data protection. These risks are especially significant in Internet use, where devices are employed that reach directly into the user's most personal sphere. Likewise, the processing of subscriber and user billing and commerce data, which is necessary for electronic communications to operate, must be shored up with all necessary guarantees to ensure that it does not have a detrimental impact on the sphere of privacy.

This sort of data processing calls for a change in the legal framework that regulates the right to data protection; now legislation must make provisions not only for natural persons, but also, in certain cases, for legal persons or corporate entities, as well as information that national and international personal data protection regulations do not traditionally address closely enough.

From the standpoint of the agents involved in the realm of electronic communications, taking measures to guarantee secure network use and the right to protection for the data of service users and subscribers takes on special importance, not only in terms of compliance with the regulatory framework, but also as a guarantee of the agents' own image and solvency in the eyes of their clients and society at large.

As a consequence, it is necessary to establish a regulatory framework that guarantees the adequate introduction of security measures in electronic communications networks, a framework that most of all recognises and expressly specifies the rights of subscribers and users in relationship with the protection of their personal data. Furthermore, it would be advantageous if agents were to offer products or services that guarantee anonymity in the use of electronic communications whenever possible.

Furthermore, if a comprehensive guarantee of subscriber and user rights is to be achieved, the different agents involved will be playing an essential role, setting up self-regulation systems to complement the aforementioned regulatory frameworks and establishing a stabdard international framework on the protection of the rights of the subscribers and users of electronic communications services.

V. THE COMMERCIAL SECTOR AND THE USE OF INFORMATION FOR MARKETING PURPOSES

Marketing is and continues to be one of the challenges of personal-data protection at present. The area's development reflects the shortcomings that can be found in standards for the protection of data at the global level. To change this, it would help greatly to establish regulatory frameworks that guarantee that personal data are used adequately for advertising and marketing purposes and to set up supervisory authorities to watch over citizens' rights.

The current stage of marketing evolution is oriented towards the generation of better and better added-value services, which at the same time can inflict serious harm on the right to data protection. Foremost among these risks is consumer profiling, which is done by comparing and integrating different types of data gleaned from a huge variety of sources without transparency or information for the data subject. In reaction to this sort of behaviour, people have begun to use self-protection techniques such as refusing to engage in e-commerce, which are having serious economic consequences. The problems are compounded by the difficulty of differentiating between media directly related with the Internetnet and new communications media that can also access online services over the telephone.

For adequate protection of personal data in the marketing realm, the participants stress the need to employ tools that render the user anonymous for all purposes other than the internal management of the products or services the enterprise offers, together with informed consent; transparency and decision-making ability; seals of authenticity and quality that can be allied with

a process of computer auditing of the quality of the services rendered by a given enterprise, the proactive practice of data protection and especially the principle of proportionality; and the use of privacy policies by the same enterprises that offer services.

Obviously, the commercial sector, including the subsector of marketing, is one of the sectors in gratest need of legislative developments and codes of standards or conduct. Such codes are rules of professional behaviour or good practices, and they are a fine instrument for boosting the adequate processing of personal data, because they complement or implement already existing regulatory frameworks.

It is in the nature of codes of standards or conduct to contribute to the correct application of the existing general regulatory framework on personal-data protection to the special features of a specific sector; furthermore, publicising such codes for general knowledge and submitting them to supervisory authorities for review are also commendable steps. 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 information society and e-commerce, commercial and promotional communications must comply with certain requirements in order to be regarded as adequate processing of personal data. One such requirement is that they must state their commercial purpose and name the natural or legal person on whose behalf they are sent. The modern tendency seems to focus on opt-in arrangements based on the prior consent of the service user.

Another indispensable factor in commercial and promotional communications is the preservation of the possibility of revoking consent whenever the data subject sees fit. One point of special importance here is the data subject's right to object, on request and free of charge, to the processing of data concerning him or her, in which case all processing of that data must cease and all processing information on that data must be cancelled, simply at the data subject's request.

Within the commercial sector and the use of information for marketing purposes, the legal framework of personal data protection is and must continue to be the framework within which information security is increased, resources are rationalised and client trust is made to grow, through adequate processing of client data.

VI. CONSIDERATIONS ON THE DEVELOPMENT OF THE IBERO-AMERICAN DATA-PROTECTION NETWORK

As a corollary of the events that breathed life into the La Antigua Declaration in the wake of the Second Ibero-American Meeting on Data Protection, one outcome was that the participants in the Second Ibero-American Meeting on Data Protection agreed to create the Ibero-American Data-Protection Network.

The Network was therefore created as a forum open to all Ibero-American countries, with the remit of boosting initiatives to share their experience and reinforce their continuous mutual cooperation in the matter of data protection.

The task of coordinating the Network was delegated to a Presidency and a Permanent Secretariat, which were held temporarily by the Spanish Data Protection Agency, with the goal of settling the matter during the Third Meeting.

The commitment made in the La Antigua Declaration was ratified at the highest level by the Heads of State and Heads of Government of the Ibero-American countries during the Eighth Ibero-American Summit held in Santa Cruz de la Sierra, Bolivia, on the 14th and 15th November 2003. Indeed, in paragraph 45 of the Santa Cruz de la Sierra Declaration, the participants stressed their acknowledgement that the protection of personal data is a fundamental right of people and highlighted the importance of Ibero-American regulatory initiatives on protection for citizen privacy contained in the La Antigua Declaration creating the Ibero-American Data-Protection Network, open to all the countries in the Ibero-American community.

This explicit, unequivocal acknowledgement lends important support to the Network's labour in mutual cooperation and all the legislative initiatives presently on the drawing board. It also gives a decisive push towards the creation of new draft legislation guaranteeing the right to protection of personal data in Ibero-America.

In this initial phase, the Ibero-American Data-Protection Network has been characterised mostly by work aimed fundamentally at providing information, a joint activity that has been largely useful for understanding the legislative reality in each country and the problems and challenges facing us in personal-data protection, as highlighted in the Santa Cruz de la Sierra Declaration.

Nevertheless, the Network's tasks, according to its charter and the encouragement offered by the Summit of Heads of State and Heads of Government, can aspire to much more, and so its structure must evolve into a proactive state where initiatives can be embodied in more concrete activity.

With this idea in mind, the reflections stated in the Third Meeting have led to the following measures concerning the Network, which are more in line with the importance that the Summit has acknowledged the Network as having, and which are incarnated in the following new tasks and strategic decisions:

a) Creation of working subgroups open to any members of the Network who are interested.
   During the III Meeting, subgroups were set up for the analytical study of the following issues:

   - Electronic government and telecommunications, at the initiative of the Chilean delegation, which shall coordinate the subgroup.

   - Access to public information and data protection, at the initiative of the Mexican delegation, which shall also coordinate the subgroup. The representatives from Costa Rica and Peru have already stated their intention to participate.

   - The Network's strategy, at the initiative of the Colombian delegation, coordinated by the delegation from the Spanish Data Protection Agency. The delegations from Costa Rica and El Salvador have already indicated their intention to participate.

   - The viability of creating Supervisory Authorities in the Ibero-American environment, at the initiative of El Salvador and coordinated by the Argentine delegation.

b) Periodic briefing on national legislative developments, including the leading pertinent court decisions as well, and the publication of the speeches and findings of the Meeting on the web page of the Spanish Data Protection Agency, in the section devoted to the Ibero-American Network.

c) Creation of a *pro tempore* Secretariat to organise Meetings, made up of the Spanish Data Protection Agency and delegations from the host countries of the upcoming meeting and the last meeting.

d) Beginning preparations for the Fourth Ibero-American Meeting on Data Protection, which the representatives of Costa Rica offered to host in their country in 2005. Preparatory work was assigned to the *pro tempore* Secretariat, which is made up this time of the Spanish Data Protection Agency and the delegations from Costa Rica and Colombia.

e) It was resolved that the Network Secretariat and Presidency for the next two years shall remain in the hands of the Spanish Data Protection Agency, and the following logotype was approved for the Network:

Cartagena de Indias, 28th May 2004