MATERIALES DE REFLEXIÓN

Proceedings of the First European Congress on Data Protection

Madrid, 29-31 March 2006

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

cámaras

Fundación BBVA

PROCEEDINGS OF THE FIRST EUROPEAN CONGRESS ON DATA PROTECTION

PROCEEDINGS OF THE FIRST EUROPEAN CONGRESS ON DATA PROTECTION

Madrid, 29-31 March 2006

Fundación BBVA

PUBLISHED BY:
Fundación BBVA
Plaza de San Nicolás, 4. 48005 Bilbao

ISBN: 978-84-96515-41-3
LEGAL DEPOSIT NO.: M-17.317-2008

TYPESETTING AND LAYOUT: Efca, S. A.
PRINTED BY: Rógar, S. A.

Printed in Spain

The books published by the BBVA Foundation are produced with 100% recycled paper made from recovered cellulose fibre (used paper) rather than virgin cellulose, in conformity with the envorinmental standards required by current legislation.

The paper production process complies with European envorinmental laws and regulations and has both Nordic Swan and Blue Angel accreditation.

Contents

Part II
THE DATA PROTECTION DIRECTIVE AND GLOBALIZATION: THE SIGNIFICANCE OF THE DIRECTIVE

Part III
DATA PROTECTION AND ECONOMIC ACTIVITY: BINDING CORPORATE RULES

Part IV
DATA PROTECTION AND THE FIGHT AGAINST FRAUD

Part V
DATA PROTECTION AND THE FIGHT AGAINST TERRORISM AND ORGANISED CRIME

Part VI
DATA PROTECTION AND TRANSPARENCY: DEVELOPMENTS IN TELECOMMUNICATIONS AND PRIVACY

Foreword

The present volume is an edition of the proceedings of the First European Congress on Data Protection, held in Madrid between March 29 and 31, 2006.

This event was organised by the Spanish Data Protection Agency, the BBVA Foundation and the Superior Council of the Chambers of Commerce, Industry and Shipping under the presidency of honour of Their Majesties the King and Queen of Spain, and with a committee of honour comprising the Minister of Justice, the President of the European Parliament, the Vice-President of the European Commission and the three senior officers of the organising institutions.

For the first time, the heads of European data protection authorities, experts on the subject matter and informed representatives from the worlds of politics and business, not just in Europe but also the United States and Latin America, came together under one roof to participate in what is intended to be an open forum for the sharing of knowledge and experiences among all agents, public and private, involved in safeguarding the fundamental right that is data privacy.

In effect, the public at the First European Congress on Data Protection had the opportunity to exchange information and join in debate about some of today's key issues in personal data protection. One such discussion revolved around

the regulatory development of the Spanish Data Protection Act, with participants dissecting the main novelties of the text, at that point still in the drafting stage.

Time was also given over to analysing the implications of the EU Directive on data protection, with reference to the work being carried out by the Article 29 Working Group and the legal framework for data protection beyond our frontiers.

Another topic for analysis was the Binding Corporate Rules and their application to private-sector economic activity, in particular their effects on business operations and the treatment to be given to international data transfers within multinational groups.

Data protection is closely bound in with the fight against fraud. In this respect, the meeting looked at the latest European proposals to combat fraud in the financial sector and its impact on privacy and, therefore, the protection of personal data.

Likewise, the legal instruments developed to fight terrorism and organised crime were examined from a data protection standpoint, with discussion centring on the changes introduced by new legal rules on the retention of data traffic.

Finally, thoughts were exchanged on how transparent government can be kept compatible with the fundamental right to data protection and the rapid development of information and communications technologies, with all the risks that this entails for the privacy of personal data.

In closing this foreword, we wish to express our thanks to all those involved in the organisation of the First European Congress on Data Protection and in the preparation of this volume, which we are convinced will do much to reinforce citizens' fundamental right to personal data protection.

Madrid, March 2007

ARTEMI RALLO LOMBARTE
Director of the Spanish Data Protection Agency

FRANCISCO GONZÁLEZ RODRÍGUEZ
President of the BBVA Foundation

JAVIER GÓMEZ NAVARRO
President of the Superior Council of the Chambers of Commerce, Industry and Shipping

Inaugural Address

Juan Fernando López Aguilar
*Minister of Justice, Spain**

It is an honour to inaugurate the proceedings of the important European Conference on Data Protection held for the first time in Spain. The purpose of the exercise is none other than protection of one of the fundamental rights that is subject to most pressure in our era, characterized by ease of access to information and its disclosure: the fundamental right known in comparative law as privacy.

Above all I wish to extend a welcome to the unique and excellent list of world experts that have gathered thanks to Professor Piñar Mañas, Director of the Spanish Data Protection Agency.[1]

And here I should offer special recognition to Professor Stefano Rodotá, Ordinario di Diritto civile Universidad La Sapienza-Roma, whose accomplishments I have followed with particular interest, during his time as a member of the Italian Parliament from 1979 to 1994 and as a member of the European Parliament in 1987. To the foregoing we add his status as Data Protection Officer in Italy until 2005, in which position he became one of the architects of European data protection policy.

---

* Position held at the time of the event.—Ed.

[1] Position held at the time of the event.—Ed.

In Spain, personal data protection is a fundamental right recognized in article 18.4 of the Spanish Constitution. It provides that "the law will limit the use of informatics to guarantee the reputation and personal and family privacy of citizens, and full exercise of rights."

The Constitutional Court, in its important judgment 292/2000 of 30 November 2000, defined the scope of this fundamental right. It established its specific and autonomous nature as the right to reputation, personal and family privacy and image, recognized in section 1 of the aforementioned article 18 of the Constitution. In accordance with the judgment, this fundamental right gives the holder a set of powers, connected with the power to require third parties to behave or not behave as specified in the law.

The Charter of Fundamental Rights of the European Union also makes personal data protection a fundamental right. In this regard its article II-68, specifically related to this right, provides that "everyone has the right to the protection of personal data concerning him or her," and that "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified," finally providing that "compliance with these rules shall be subject to control by an independent authority."

Also within Europe, the proposed treaty that would establish a European Constitution includes in its art. II-7 everyone's right of privacy, and art. II-8 provides that "everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

Organic Act 15/1999 of 13 December 1999 on Protection of Personal Data (LOPD) is the law governing this fundamental right. It also implements 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.

The basic objective of the Organic Act is to guarantee and protect, in relation to the processing of personal data, the public freedoms and fundamental rights of individuals and, in particular, the right to protect their reputation and personal and family privacy. For this purpose it establishes and regulates a series of rights of data subjects, as well as the correlative obligations of data controllers.

It must be noted that the safeguards that the Act establishes regarding the rights of individuals have been relatively affected by the understandable absence of regulatory implementation. Since 1999, when the Act came into force, the need to draft implementing regulations was obvious to all.

The work and studies necessary to draft them did not commence until the middle of 2004. They took into account the comments made by the European Commission on the Act implementing the directive in Spain, in order to achieve total harmonization of the two texts. They also took into account the interpretation the Commission had made of its provisions over the nearly 10 years it had been in force.

The Spanish Data Protection Agency (AEPD), the independent public entity to which the LOPD assigns the task of supervising compliance with this law, has been taking this interpretation into account in the resolutions, reports and orders issued in the performance of its duties. It has also followed the recommendations prepared by the Working Party for Article 29 of the directive, of which the Director of the AEPD is currently Vice Chairman.

At this moment I can reveal that the proposed regulations are in a very advanced state of preparation and are expected to come into force during the first half of 2007.

Once the new regulations come into effect and a reasonable period of time has passed for observation of their positive effects on safeguarding and defending this fundamental right, it will probably be appropriate to consider the possibility of amending the Organic Act. This possible initiative could consider enhancing protection of the right, and regulating the manner by which data subjects give consent to the processing of personal data.

In any event, the time that has passed since the first Personal Data Protection Act has brought a growing social acceptance of the regulation of this right. Thus, the business sector, far from considering the obligations deriving from the LOPD to be a burden, views them as an element of improvement of corporate management and customer relations. Indeed it is worth noting that some of them believe adopting an appropriate privacy policy has a positive impact on their image.

To the foregoing we would add that, to the extent that the LOPD has been implemented in our society, awareness and approval of new Model Codes has grown, as was contemplated by the Act. These Codes are in the nature of ethical or good practices codes, the purpose of which is to facilitate application of the Organic Act in given sectors.

The problems related to effective application of the data protection regulations were analyzed by the European Commission in its May 2003 First Report on application of Directive 95/96/EC.

It cites the need to develop stronger coercive action to improve application of the legislation. The expected effect of this action is that data controllers will provide more and higher quality information to data subjects regarding the processing they undertake and the data subjects' rights. This would result in a greater degree of awareness of data protection among the citizenry.

In this regard I must state my confidence and optimism in the potential shown by the Spanish model. In Spain we not only have an Act that provides high standards of personal data protection, but also an entity, the Data Protection Agency, which has the human and material resources, and the necessary authority, to suppress conduct contrary to the rights of citizens, and also to impose sanctions at a high level.

It is for this reason that I express my satisfactory view of Spanish regulation in this unique area, the protection of personal data. This of course does not mean that we have nothing more to learn. We must be open to and learn from experiences and structures prepared in other countries. We must pay attention to the evolution of technological developments and the new security requirements resulting from certain anomalies of current society. Among others, these include terrorism and organized crime, the transparency of financial markets, immigration and electronic government.

For the reasons set forth above, I welcome the initiative to hold the First European Congress on Data Protection in Spain. The presentations and debates will allow deeper knowledge of the problems and guide us to the right solutions, always bearing in mind the need to balance all of the lawful interests involved and make them compatible.

The conference schedule has wisely chosen the most burning questions of the moment. These are the relevance and meaning of data protection regulations, starting from perhaps the most developed model in the entire world, the regulations established under the European Personal Data Protection Directive, and complementing it using the perspective of other geographic areas such as Latin America, the French-speaking world, the United States of America and Canada.

Closely related to the purpose of Directive 95/46/EC to promote a harmonized environment for protection of personal data that eliminates obstacles to international trade, there is a debate regarding one of the most novel legal instruments for achieving this objective; binding corporate rules in the large multinational groups operating in various countries. In this regard, we are analyzing mechanisms allowing us to give them binding legal force, so that the greater flexibility they offer for making international transfers of data is matched by adequate safeguards for individuals and public authorities.

I would like to state my certainty that the conference will stimulate debate regarding the balance between personal data protection and the need to confront new forms of crime. Standing out in this regard are Internet fraud, with specific impact on the financial sector, money laundering and terrorism. I am also certain that it will help in establishing appropriate regulations to the Organic Act on Personal Data Protection, a task the government has pledged to complete during this legislative session.

Finally, I would like to conclude by thanking the Director of the Spanish Agency, José Luis Piñar Mañas, for his decision to take the initiative in inviting the excellent list of experts that has gathered for this conference and, ultimately, for the diligent work and care he has exercised in leading the Agency, earning it respect not only internally but also on an international basis.

Privacy and the Future: Some Opening Reflections

Stefano Rodotá
Professor of Private Law and Former Data Protection Officer in Italy

We live at a time when personal data protection is characterized by great contradictions, if not true social, political and institutional schizophrenia. Awareness of its importance is ever greater, not only as regards protection of the private lives of individuals, but also protection of their freedom. That said, it is increasingly difficult to respect these elements, because requirements of internal and international security, market interests and reorganization of public authorities are pushing for reduction of the guarantees.

What should we expect in the future? A continuation of the trends that have emerged on a preliminary basis over recent years, or a reactivation, albeit laboured, of the logic underlying personal data protection which, with great clairvoyance, has opened a new era for protection of freedom?

To understand the present, and look to the future, we must be aware of the past. Europe has reactivated and renewed the modern concept of privacy as developed in the United States. Let's review the most significant passages from this history. Self-determination regarding disclosure of information was recognized as a fundamental right by the Bundesverfassungsgericlit in 1983. In 1995, with European Directive No. 46, it was explicitly stated that the harmonization of laws should not have "the effect of weakening the protection they give, but rather the

aim should be to assure a higher degree of protection." In the year 2000, with the Charter of Fundamental Rights of the European Union, the protection of personal data was recognized as an independent right, thus contributing to the "constitutionalization" of the person, which the Preamble to the Charter places "at the centre" of the Union's action. This line has had significant institutional results, such as the two notices by which the European Commission has established that its legislation and regulations must always be submitted to a preliminary review for compatibility with the Charter of Fundamental Rights. Also, within the European Union, personal data protection has passed from the Internal Market sector to the Freedom, Security and Justice sector, with explicit acknowledgment of the fact that we now are dealing with a matter that cannot be reduced to mere economic logic, but rather goes to the rights and freedom of individuals.

The institutional framework thus appears to be encouraging. But reality is ever more removed. There are three main reasons for this new course.

First: since 11 September many reference criteria have changed. Guarantees have been reduced. This is shown in particular by matters under the Patriot Act in the United States and European decisions regarding transfer to the United States of airline passenger data and retaining personal data regarding communications.

Second: this trend to reduce of the guarantees has extended to sectors, such as economic activities, that attempt to take advantage of the change in the general climate.

Third: the new technological opportunities offer ongoing and growing instruments for classification, selection and tracking of persons. This is resulting in an independent derived technology that even the national and international authorities do not always appropriately monitor.

In this manner, there is an erosion of some principles upon which the personal data protection system has been constructed, in the first place the principal of finality and the principal regarding separation of data processed by public bodies and those processed by the private sector. The trend is to impose, even using institutional pressure, the multi-functionality criterion. Data collected for a given purpose is made available for other purposes, considered to be as important as those with respect to which the collection was justified. Data processed by one company is made available to others.

Reuse and interconnection concepts prevail, almost always justified by arguments of efficiency and economy. If all databases are connected, the public authorities can serve citizens more rapidly, at lower cost and with less inconvenience

for the interested parties. If information collected by the private sector, courts and police can also be accessed, terrorism and crime can be better fought. If data regarding Internet access, the music industry and movies can be accessed, we can more easily discover who illegally downloads music and films.

But adopting such logic not only contradicts principles essential to data protection, but also breaks the compact with the citizenry in an area that is ever more essential to effective protection of their freedom. They have been promised that data must be processed by the public authorities for specific purposes identified by law, and by the private sector only with the consent of those involved, who in this regard can precisely limit the lawful use of the information collected.

A very significant confirmation of abandonment of these principles has been received from the US government, which has requested Google data, including cumulative data, regarding access to certain sites, justified by the fight against paedophilia. The logic underlying this request is very clear: the irrelevance of the purposes for which a database has been formed; the resulting availability of the data for any use considered to be important to achieving the public interest; the cancellation of the boundary between public and private databases. This shows a new dimension of surveillance, which exalts the power of the State to use any personal information, whoever collected it and regardless of the original purposes for the collection. The whole of data processed by private parties is treated as a resource available to the public authorities.

Thus absolute power is asserted for the State to place its hands on the "electronic body" of citizens. The reaction should be a strong assertion of "habeas data" giving the electronic body the protection that habeas corpus for 800 years has given the physical body, reacting to the absolutist claims of the king. The "constitutionalization" of the person, visible at least in the system of the European Union, requires us to move in this direction. The breakage of the scheme founded on the principle of finality and the force of consensus also is a result of a more general trend toward extension of information collections to an ever greater number of persons. We are moving from collection for a purpose to generalized collection. The universe of persons subject to monitoring is expanding and not only individuals or groups considered to be dangerous: currently the entire population is considered to be "a potential dangerous class" or just a group of mere consumers, which justifies the creation of "total" collections of data, the incessant production of individual, family on group profiles based on information that also covers health, financial status, and cultural choices.

These mass collections of personal data already have resulted in transformation of all citizens into potential suspects in the eyes of the public authorities,

and in individuals being objectified by the systems maintained by companies. In addition, the growing possibility of public authorities interconnecting all of their databases and obtaining information from any private source results in unprecedented social transparency, which changes the position of citizens in democratic societies and their relationships with the State.

Thus "nations of suspects" are created, and the citizen is demoted to the status of a consumer. The crowd no longer is "lonely," as described by David Riesman. It is now "naked," continuously monitored by security technologies or by the explosion of electronic cards recording all of its movements, preferences and aptitudes. It has become a body available for the creation of databases where, for example, genetic information is also collected to be monitored from birth for the entire population or significant segments, for purposes of prevention of certain diseases, but also in order to monitor possible development of a tendency to violate the law by those having family histories of criminal background. The individual in this way is deprived of the right to freely build his future.

All of this results in significant changes in the overall framework within which data protection had been placed, and raises problems as regards the possibility of planning for the future. There are at least two reasons. The protection of personal data was conceived more as a defence of individual freedom, but now it is becoming increasingly evident that it is urgent that we protect group freedom related to the maintenance of the democratic nature of our societies. Above all, the new frontiers of data protection go directly to the bodies of persons, which have drawn growing and often disturbing attention.

The body assumes the leading role. A manipulated body is appearing, predisposed to control, locatable. The impact of the technology in effect is directly on it. Control over it is not limited to external monitoring, as occurs for example with video surveillance. It is not limited to using natural characteristics, as occurs when using biometric data. By contrast, it is accompanied by electronic devices, in the first place those related to RFID technology. It is integrated and modified by the insertion of electronic implants and, prospectively, nanotechnologies. It transforms it on a global basis, not only becoming post-human or trans-human, but affecting the very independence of individuals, who may be remotely monitored and managed. The body thus becomes a new object, which gives a new meaning to what today is personal data, to allow the previously contemplated protection to continue to function.

The specific examples are before us. Every day there are more. Very well known are cases of workers who are required to carry a small "wearable computer," agreeing that the provider of work may, via satellite, manage their work, lead

them to the products they are to pick up, indicate routes to be taken or activities to be undertaken, monitor all movements of the employee and thus at all times know where they are. In the 2005 report of Professor Michael Blackmore of the University of Durham, requested by the English union GMB, it is noted that this system already involved 10,000 persons, transforming workplaces into "battery farms" and creating conditions of "prison surveillance." What we have is a Panopticon on a reduced scale, which anticipates and announces the possibility of spreading these forms of social surveillance on an ever greater scale. Similar results, although only regarding location within worksites, are currently possible thanks to the insertion of a readable chip using RFID technology in employee identification cards.

At the beginning of this year an Ohio company, City Watcher, went even further in manipulation of the bodies of its employees, requiring some of them to implant a microchip in the shoulder in order to be identified at the entrance to reserved premises. The very physical nature of the body is so modified, predisposed for direct control. The technique of insertion in the body of microchips that are remotely readable is spreading to the most diverse sectors, from discotheques to hospitals, to the opening of doors of houses or one's personal computer, with decreasing costs and increasing ease of implantation.

In some countries, such as Italy, application of these technologies is prohibited when it results in remote control of workers. It is not sufficient to propose that this prohibition be generalized and become a common rule in the countries of the European Union. These technologies also are used for individuals and activities apart from those that are work-related, the lawfulness of use of instruments that imply manipulation of the body should be addressed directly. In the 2005 view of the European Commission's Group for ethics in sciences and new technologies regarding electronic implants in the human body, it was concluded that the use of microchips was permitted only to protect the health of the person involved. It was believed that other uses should be considered to be contrary to the dignity of the person, declared inviolable by Art. 1 of the Charter of Fundamental Rights of the European Union, and to the principle of protection of personal data.

What in fact will a society become if a growing number of persons are tagged and tracked? Social surveillance would be entrusted to a kind of electronic collar. The human body is like any moving object, remotely controllable via satellite technology or using radio frequencies. If the body may become a *password*, localization technologies will be creating a *networked person*.

Before us are mutations that affect the anthropology of beings. What we have are progressive transitions: from a person "scrutinized" using video surveillance

and biometric techniques we may progress to a person "modified" by the insertion of "intelligent" chips and tags, in a context that identifies us on an increasing basis as "networked persons," persons perennially on the network, and bit by bit configured to issue and receive signals they consent to using, reconstructing movements, customs, contacts, and thereby modifying the feeling and content of independence of persons.

The derivative technologies thereby acquire particularly disturbing features. Can the purposes of identification, verification, surveillance and certainty in transactions really justify whatever use of the human body is made possible by technological innovation?

These considerations obviously are also applicable in those cases of RFID technologies that that do not result in modification of the person's body. To examine this kind of problem, it is necessary to distinguish those cases in which the tags are used as instruments directly related to a person (for example the content of an identity card) from those in which the relationship derives from a relationship with objects, also tagged. In the first case surely what we have are situations quite similar to those characterized by direct implantations in the body, although the person always has the possibility of removing the medium containing the tag, thus removing the control (a possibility that is impracticable or more complex with respect to implants in the body, even in those cases in which it is reversible). In the other cases, it is a matter of proceeding to adapt the current data protection system, rigorously taking into account the sensitive nature of the control and the classification that this manner of collection of data makes possible, properly emphasized by the working document approved in January by the Group in Article 29. This also implies, on the one hand, reconsideration of the definition of personal data to confront the dangerous trend to adopt formalistic and restrictive interpretations that may prejudice protection of persons, particularly (but not only) in the case of application of RFID technology. In addition, the risk that standardization procedures, making access to the data contained in the chip by multiple agencies and active processing of that data possible, will result in monitoring and manipulation of identity, must be seriously considered. In even the least worrisome cases of direct implantation in the body, the smart tags nonetheless appear to be susceptible to much broader use, and thus may result in more profound personal and social effects. Although mass use of microchip implantation may be unthinkable, it is exactly the approach adopted for many new documents. It has been learned that, in the United Kingdom, what new identity documents contain is exactly a chip readable using radiofrequency technology. If this fact is associated, for example, with the use of small pilotless airplanes (UAV: unmanned aerial

vehicle) that are being tested, police forces can identify persons participating in a demonstration or congregated in any place by overflying the area using one of these aircraft (George Monbiot so reported in "The Guardian" of 21 February 2006). Doing so affects fundamental constitutional freedoms, such as travel or free public demonstration. This makes more appropriate attention to protection of personal data necessary in this new area.

In addition, the same advantages deriving from these new technologies for certain categories of people (children, the ill, the aged, the disabled) may lead to insurance companies to condition insurance contracts or set the premiums to be paid based on the fact that such persons are "equipped" with such technology, thus reducing the risks to the insurer. This is already the case with automobiles and trucks, for which theft insurance is available on more favourable conditions if they are equipped with a device readable by satellite. But can people be made the equivalent of moving objects, with their extreme "commoditisation" [a kind of commercialization of persons]? Or would just a form of protection of personal data, preventing this manner of collecting it, be the best instrument to assure freedom and dignity?

The extreme frontier of the impact of technological innovations on the body today is represented by experiments and hypotheses regarding nanotechnologies in general and nanobiotechnology in particular. Invaded by the infinitely small, the body may undergo a radical metamorphosis, becoming a "nanomachine," a sophisticated information system uninterruptedly producing analytical data regarding its condition. Protection of this category of data requires utmost attention. It is today's problem, not tomorrow's. It also should be of interest to everyone involved in protection of personal data, in a "vision assessment" exercise.

Nanotechnology will result in very significant innovations affecting processing of personal data. Miniaturization of diagnostic instruments, their direct presence in the body of the person in question, multiplication of the parameters that may be simultaneously used, expansion of the diagnostic spectrum and huge acceleration of diagnostics will inevitably result in a vast increase in the data that are available and immediately usable. It is essential to participate from the outset in identification of the problems related to creation of this new "internal space." There are new characteristics, together with traditional questions. These include the right to know and to not know, individual and mass screening, who may have access to data produced by nanotechnology, the nature of the data, which may represent a degree of "sensitivity" even greater than the extremely sensitive genetic data, even more sharply re-presenting matters of possible discrimination.

The social and ethical acceptability of nanotechnology in good part will also depend on the possibility of accompanying its introduction with appropriate guarantees of personal rights.

This attention to a new "internal" space, and this essential look at the future, must not lead us to forget the manner in which the "external" space currently is being restructured. Here three trends may be noted, convergent and all restricting the level of data protection: trends toward completeness, permanence and availability of the information collected. The closest example we have is represented by recent European Directive 2005/182 on retention of data, which is an immediate exception regime as regards Directive 2002/5 8. It has been broadly discussed. Its rules well illustrate the questions regarding completeness (retention of all data related to electronic communications), permanence (from six months to two years, but with the possibility of the Member States extending these terms), and availability (generic reference to "serious crimes," and to "competent national authorities"). The guarantees are not adequate, beginning with what should be the most significant, relating to exclusion of data regarding the content of communications.

An example taken from the Italian experience may help clarify the scope of the problem. In Italy, every day, 800 million telephone calls are made and 300 million e-mails are sent. For one year, the total is almost 400 billion electronic communications. Since the related data is retained for at least four years (but may be retained for up to six), this means that the databases of the communications providers contain at least a 1.6 trillion items of personal data. Based just on retention of the addresses of the sender and addressee, this allows reconstruction of the fabric of personal and social relationships (how many times have I called a given person?), political and union relationships (with what organizations are they in contact?), economic relationships (with what companies and stockbrokers do I maintain relationships?), regarding religious faith (am I associated with a parish, synagogue, or mosque?). But even more delicate is retention of data related to access to Internet sites, because such access speaks more clearly of likes, preferences and inclinations. Can we accept this mass storage? Is the intended purpose proportionate with the instrument used?

And not retaining the content of communications runs the risk of becoming a boomerang, not a guarantee. If I have made an innocent telephone call to one who turns out to be a criminal, the impossibility of demonstrating the true content of the communication leaves me under a cloud of suspicion. And that suspicion may even be constructive: since attempted calls that are not completed must be recorded, someone may call me at a time when he knows that I am not

available to answer, thus creating an appearance of a relationship tying me to this person, whom I may not even know.

These new, gigantic collections of information also increase social vulnerability. Each of us is exposed to the risk that the data will reach the hands of those illegally managing to access these huge and not always overly secure databases, and that sensitive information will be circulated by unscrupulous employees of the companies managing the collections of information. It is a real risk. Last year the data of 52 million MasterCard customers was stolen. The United States Senate, aware of this danger, has approved a bill requiring database managers to advise their customers of the danger of "identity theft." The nature of data protection changes, and thereby the entire social organization changes.

But today, presence in the external space, the Internet, creates unprecedented problems regarding identity. Anonymity on the Web has been much discussed. The relationship between identity and freedom on the Web raises other considerations.

The central question is not just maintaining firm control of one's private life, but rather an obligation to live in public, a continuous appropriation by others of the flow of our lives. A new space has been created. It cannot be defined by traditional references to public and private. Often we move within it in search of ourselves, even finding bizarre information, mystification, total falsification of our identities that anyone can accomplish by placing our imaginary biography on the Web, at a particular site or in a general encyclopaedia. And the omnivorous search engines are ready to place it in everyone's hands. The right to eliminate or correct the false or imaginary information, the right to forget it by cancelling the information, may not be sufficient when the information has entered into planetwide circulation. It is said that the only realistic reaction is the creation of a site to which we deliver our true identity, in the hope that this information may be recorded and accessible from the same portals where our former or false image may be found.

Nevertheless, regarding this and other matters we cannot limit ourselves to identifying the difficulties, seeking only some "furtive hunter strategy" or even resigning ourselves to our impotence. Instead, it is possible to identify some possible strategies.

The first obviously relates to initiatives tending to expand the scope of common rules, which is most significant precisely in the European Union. Since 2000, with the Charter of Venice, the personal data protection authorities have indicated the route to an international treaty, an idea that was again considered at the last Montreux conference. A Charter of Internet Rights was again discussed last

November at the World Forum on Information Society, organized in Tunis by the UN, and this idea in January 2006 was submitted to the Civil Liberties Committee of the European Parliament. In the United States a Global Internet Freedom Act was presented to Congress in May 2005. The demand for international rules protecting freedom of expression was strengthened by the recent censure episodes initiated by Microsoft and Yahoo! regarding China, which also alarmed Reporters sans Frontiéres. The road to a global international document surely is long but it should not be abandoned. In the meantime it is necessary to continue paying attention to what is happening in the Mercosur area. And it is possible to begin initiatives regarding specific matters, for example maintaining dialogue with the United States regarding spamming, as was begun by the last European Commission, or regarding nanotechnology, as suggested by the CNIL [Commission nationale de l'informatique et des libertés].

Thus, it is necessary to again take the approach adopted by the European Parliament, which has challenged the provision regarding transfer of airline passenger data to the United States before the Court of Justice. We should begin to consider challenging national provisions applying decisions of the Commission that violate fundamental rights of citizens. It is also necessary to take seriously what the Commission has stated regarding the need for control under the Charter of Fundamental Rights of the European Union, which otherwise runs the risk of becoming a paper provision. In Whereas Clause 22 of the directive regarding retention of data, for example, based on paradoxical argument it is stated that the restriction of freedom of communication better guarantees the rights contemplated in articles 7 and 8 of the Charter. The time has arrived to begin asking the Court of Justice to monitor the validity of the manner in which the declaration is made pursuant to the Charter in the acts of the Commission.

More generally, using all the resources available and taking advantage of all opportunities, it is urgent to stop the growing contamination of the civil liberties environment resulting from a set of rules that, for various reasons, restricts protection of personal data. This is essential in order to avoid resort to scientific and technological innovations favouring the formation of a control, classification and social selection society. And this is also necessary to give technological innovations the social legitimacy that results in confidence of citizens, thus making better functioning of the business community possible.

This task is becoming ever more difficult. More and more often we ask ourselves whether protection of personal data can really survive with the goals and expectations with which it was created. Nevertheless, as Spiros Simitis has written, it

continues to be "a necessary utopia." A utopia, nonetheless, that does not lead us to view a distant future. Rather, one that requires consideration of the reality that is around us. Protection of personal data is already an element of the freedom of our contemporaries. It is not rhetoric to recall it at all times, because each of its variants affects the degree of democracy that each of us may enjoy.

Part I

REGULATORY DEVELOPMENT OF THE ORGANIC DATA PROTECTION ACT

1

Strengthening Legal Certainty: New Regulations Developing the LOPD [Organic Data Protection Act]

José Luis Piñar
Director of the Spanish Data Protection Agency[*]

Perhaps some of you are aware of the work that has been undertaken by the Agency in cooperation with the Ministry of Justice over the course of this year and part of last year, to make it possible for the Regulations developing the LOPD to see the light during this year. In particular I wish to refer to the importance and magnitude of the work that has been undertaken, and the transparency that has guided its progress. During the process there have been maximum information and dissemination to ensure participation of all the affected sectors and the public at large.

Thus in April 2005 in Madrid and Barcelona we participated in the 9th LOPD Conference, organized annually by Equifax (the entity that manages the principal information database regarding solvency and credit in Spain). This conference dealt exclusively with the regulatory development of the LOPD.

When we had a first document regarding substantive aspects of the draft regulations, in June 2005, the Agency, together with the Universidad Menéndez Pelayo, organized a monographic seminar in Santander to publicize the principal aspects of the regulations and submit them to debate, under the title "Hacia

* Position held at the time of the event.—Ed.

un nuevo Reglamento de la Ley Orgánica de Protección de Datos" ("Toward New Regulations of the Organic Data Protection Act"). The level of attendance and active participation achieved at that seminar demonstrated the great interest in the matter, among not only the business and professional sectors, but also among the citizenry, represented by various social organizations.

The speakers at the seminar were representatives of the European Commission, other data protection authorities, the Socialist and Popular parliamentary groups, consumer organizations, the disputed Administrative Chamber of the National Audience (which is the court having jurisdiction to review the resolutions of the Director of the AEPD, the Spanish Federation of Municipalities and Provinces, research centres and private companies in the advertising, marketing, insurance, telecommunications, credit, financial, technology, consulting and energy sectors.

In October we accepted an invitation from the Chairman of the Confederación Española de Organizaciones Empresariales [CEOE—Spanish Confederation of Business Organizations] to receive its comments on the text that was being worked on with the Ministry of Justice.

We also have received comments from other large organizations, such as the Unión Española de Entidades Aseguradoras y Reaseguradoras [Spanish Union of Insurance and Reinsurance Institutions], an organization of the most important companies in the sector in Spain, the Federación Española de Comercio Electrónico y Marketing Directo [Spanish E-Commerce and Direct Marketing Federation], an organization of many companies in the sector, as well as the Consejo Superior de Cámaras de Comercio, Industria y Navegación de España [Superior Council of the Chambers of Commerce, Industry and Navigation of Spain], the Consejo General de la Abogacía [General Attorneys Council] and from many other business sectors.

Of course the Consejo Consultivo de la Agencia [Advisory Committee of the Agency], which is a professional body advising the director of the agency, with representatives of the two houses of Parliament, the General State Administration, the autonomous data protection agencies (which also participated on a continuous basis in the process), the local corporations, consumers and users, those responsible for private files and the Royal Academy of History.

In addition, the Agency has participated in many events organized by various institutions, such as the Instituto de Fomento Empresarial [Business Promotion Institute], the Foro de Socios del Instituto de Empresa [Business Institute Partners Forum], in which representatives of the most important law firms in

Spain participated, the Club Financiero Génova [Genoa Financial Club] and the Fundación Universidad-Empresa de Valencia [Valencia University-Business Foundation]. All of these events were organized for the sole purpose of dealing with this matter. The sense of the regulatory development contemplated was conveyed to all participants.

I believe all of this gives a clear idea of the open and transparent nature of the work that has been undertaken. Finally, I believe I can assert, as I said before, that the AEPD has acted in a particularly transparent way regarding rules that directly affect business activity, making a significant effort of dissemination, the direct consequence of which was significant work in receiving and studying all proposals and suggestions that were made.

This attitude has been maintained even at the expense of delaying processing of the draft, which currently is in the formal process of approval by the Ministry of Justice, which legally heads the initiative.

I believe that for reasons of legal certainty it is of urgent importance to have these regulations as soon as possible. Without doubt they will contribute in a decisive way to achieving greater clarification of the range of rules in effect as of this date.

In the first place I must note the fact, truly unusual from the point of view of legislative technique, that the LOPD does not include a statement of purpose, which has a very significant impact on the task of application and interpretation of its substantive provisions.

In addition, it has no regulatory rules specifically developing its content. We know that currently the regulatory rules that were issued in development of prior Act 5/1992 of 29 October 1992, regulating the automated processing of personal data (the "LORTAD") are in effect, to the extent they are not contrary to the LOPD, as provided in its third transitional provision.

Specifically, these regulatory rules are Royal Decree 428/1993 of 26 March 1993, approving the Bylaws of the Spanish Data Protection Agency, Royal Decree 1332/1994 of 20 June 1994, developing certain aspects of the LORTAD, and Royal Decree 994/1999 of 11 June 1999, approving the Regulations for Security Measures for Automated Files that contain personal data, in addition to the Instructions issued by the Agency in application thereof.

The referenced rules, in addition to predating the LOPD, are dispersed and cover only partial aspects of the Act. For that reason, they in no way provide a sufficient and global regulatory context for the subject matter.

Therefore there are many aspects of the LOPD the precise outlines of which have been set over the term that they have been in effect, both by decisions adopt-

ed by the AEPD and by judgments issued by the courts, both the National Audience and, to an increasing extent, by the Supreme Court.

As regards to the AEPD, this entity in the exercise of its authority regarding application of the law, by means of resolutions issued in the various proceedings handled and through legal reports issued with respect to inquiries presented by file and processing controllers, has been establishing criteria and clarifying certain aspects, by means of interpretation of the applicable legal rules.

Nevertheless, obviously, this is not sufficient. The task of complementing the provisions of the LOPD through the corresponding regulatory rules over the years has become a real necessity. We must attend to it on a priority basis in order to provide the necessary legal certainty to those to whom the law applies, and adapt its provisions to current conditions, very different than those existing in 1999.

In this regard, we cannot ignore a whole series of *decisive factors:*

— The *growing importance of the personal data protection right* expressly existing since Constitutional Court Judgment 292/2000 of 30 November 2000, as I said at the beginning of this presentation, as a fundamental right separate from the right of privacy, which is also so recognized in the European Charter of Fundamental Rights proclaimed in Nice on 8 December 2000, and in the Draft Treaty establishing a European Constitution, which recognizes it in two places: in its Part II, which incorporates the Charter of Fundamental Rights of the Union, and in its Title IV, regarding "the Democratic Life of the Union."
— The *unceasing daily development of information technologies,* which imposes a need to adapt the legal provisions then established regarding procedures and requirements for matters such as a means of providing information or obtaining consent, to name just two of them.
— *Globalization,* with the consequences deriving therefrom regarding international movements of data.

For all of the above reasons, I believe it is absolutely necessary to have LOPD regulations that include a clear and detailed statement of purpose to remedy the indicated absence of a preamble for the Act. Approaching regulation of the subject matter on an overall basis, it must end the existing dispersement of rules, at the same time providing greater transparency contributing to dispel the doubts that have arisen regarding application of the rules as a result of their varying regulatory hierarchy (Royal Decrees, Instructions of the AEPD). It must correct cer-

tain deficiencies in the structure of the LOPD itself, to help lessen the doubts that have arisen regarding interpretation of Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Regarding *substantive regulation* of this fundamental right, the need for LOPD regulations is obvious if we take the following into account:

- In the first place, the regulations will include development of the provisions appearing for the first time in the LOPD which, therefore, are not included in the prior LORTAD or its developing regulations. This would be the case of regulation of certain matters related to non-automated files, not included within the scope of application of the prior Organic Act. In particular it would include the security measures applicable to such files, and the regulation of the right of opposition, to cite two specific cases. I will refer to them in more detail later.

  Although the precise meaning of these provisions of the LOPD that I refer to has been addressed by opinions of the Agency itself and in court cases, it is clear that specific development thereof is demanded by the principle of legal certainty.
- In the second place, the regulations without doubt will contribute to clear specification as to which provisions have been repealed and those that remain in effect.

  Again the paradigm example is application of security measures to non-automated files. The transitional effectiveness of the regulatory rules developing the LORTAD I referred to above, "to the extent not contrary to the LOPD" requires an exercise of harmonized interpretation of the LOPD and the regulations developing the LORTAD to determine what provisions of those regulations are contrary to the rules of the LOPD. The effect of this interpretation on the principle of legal certainty, as we will see, is the root cause of the need to implement the developing regulations we are considering at this seminar.
- In the third place, we must not forget that, based on decisive Constitutional Court Judgment 292/2000 of 30 November 2000, expressly recognizing the fundamental right of data protection as an autonomous right separate from the right of privacy, the regulations could establish the legal regime applicable thereto, to that fundamental right, which would affect the definition of its scope and the principles, rights and obligations related to it.

- In addition, the regulations would incorporate precedents now appearing in the resolutions, reports and recommendations of the Agency and the judgments of the National Audience and the Supreme Court, which have answered some questions that have raised problems in practical application of the Act.

First it is necessary to emphasize that the draft regulations make the principle of finality the basis of all rules regarding data protection.

This having been said, I will now refer to the *most relevant questions* regarding the draft that has been prepared:

a) *Clear specification of the scope of application*

"Regarding the substantive scope of application, I have already referred to the question of application of the LOPD to both automated and non-automated files and data processing. In this regard, in addition to the resolutions issued by the AEPD, the 19 May 2004 Judgment of the Disputed Administrative Branch of the National Audience is instructive. It makes it clear that the Act fully applies to any non-automated processing occurring after its effective date.

This judgment rejected an appeal filed against an Agency resolution of 25 March 2002, for violation of article 10 of the LOPD. The appellant argued that the LOPD does not apply to non-automated files and processing, under the fourth additional provision of that Act. The case involved a document manually generated using data provided by the complainant. It must be noted that the document was generated after the effective date of the LOPD.

As indicated in the judgment, the LOPD is applicable to both automated and non-automated files. The judgment adds that the appellant in any event could not seek protection in the period for adaptation, because the first additional provision refers to files created prior to the effective date of the Act. In this case, the complainant's personal data were collected after that date.

The regulations also will specify what is meant by files related to personal and domestic activities. They will take into account case law deriving from the important judgment of the Court of Justice of the Communities of 6 November 2003 (the Lindqvist Judgment). Pursuant thereto, only processing related to activities within the framework of the private or family life of individuals is considered to be related to personal or domestic activities."

In addition to specifying the substantive scope of application, the regulations will clarify the *territorial scope* of application of the LOPD, clarifying it in the light of the provisions of art. 4 of the directive, so the Act will be applicable to process-

ing undertaken "*within the framework of the activities of an establishment of the processing controller, provided that it is located within Spanish territory.*"

b) *Definition of certain concepts*

The regulations will incorporate definitions of certain terms, the lack of clear definition of which in the LOPD in practice has raised problems of interpretation. This is the case of certain expressions used in the Act such as "incompatible purpose," used to regulate the principle of quality of data, "health-related data" and "sources accessible to the public," to note a few.

Incompatible purposes

As we know, article 4.2 of the LOPD provides that "personal data subject to processing may not be used for purposes incompatible with those for which the data were collected."

This expression has raised certain doubts regarding its exact meaning. In this regard I would like to refer to the judgment of the same branch of the National Audience of 11 February 2004. It established the need to obtain consent for the use of usage and invoicing data for marketing purposes, in the telecommunications sector. In this case, the court indicated that article 4.2 of the LOPD must be interpreted in the sense that "when data are used for a different purpose consent of the data subject is required."

Health-related data

The LOPD establishes a special protection system for certain categories of data based on their special nature. I am speaking of the data referred to in article 7. It covers data that reveal ideology, union affiliation, religion and beliefs, data referring to racial origin, health and sex life, and data regarding commission of criminal or administrative offences.

Of such data, health-related data in practice have resulted in the greatest problems regarding scope and content, since the LOPD does not define health data.

Nevertheless, various resolutions of the Agency have addressed this issue. Doctrine has been developed based on the definition of health-related datum contained in section 45 of the Explanatory Report for Council of Europe Convention

108 on protection of rights of individuals concerning processing of their data. It holds that the concept covers "information concerning past, present and future health, physical or mental, of an individual," and may relate to information regarding an individual who is in good health, ill or deceased. In addition, it adds that "such data must also be understood to include information regarding alcohol abuse and drug consumption." Also taken into account in this regard was Recommendation No. R (97) of the Council of Ministers adopted on 13 February 1997, on protection of medical data. It provides that the expression "medical data" refers to all data of a personal nature regarding the health of a person, and also data manifestly and closely related to health, as well as genetic information.

In this regard, we also have contributions of interest provided by the case law of the Court of Justice of the European Communities, such as the Lindqvist Judgment of 6 November 2003. As. C-101/01. It indicates that "taking into account the purpose of this directive, it is necessary to broadly interpret the expression 'health related data' as used in its article 8, section 1, so that it includes information related to all aspects, both physical and psychic, of the health of a person." Therefore, the Court holds "that the indication that a person has injured a foot and is in a status of partial medical leave is a personal datum related to health in the sense of article 8, section 1, of Directive 95/46."

Sources accessible to the public

The definition of the concept of "sources accessible to the public" is a question of great importance and significance. It requires the greatest possible precision. For this purpose the regulations would be a particularly suitable instrument as there are certain deficiencies in the Act.

In this regard, the structure of the definition contained in art. 3.j) has been corrected, emphasizing the exhaustive nature of the list of sources accessible to the public.

Nevertheless, the concept of service accessible to the public also has been clarified in an expansive manner.

Thus, it has been provided that reference to "telephone books" in the Act must be understood to refer to "electronic communications services guides," adapting the concept to the provisions of the legislation for the telecommunications sector and article 28.4 of the LOPD. Thus, not only data contained in telephone books but also those contained in such other electronic communications directories as may be prepared may be processed.

Regarding lists of persons belonging to professional groups that contain certain data regarding them, it is clarified that sources accessible to the public may include lists other than those prepared by professional associations, and that the professional address datum must be interpreted to include both the postal address and other information regarding telephone or fax numbers and e-mail addresses.

c) *Establishment of uniform rules for computation of terms for various procedures contemplated in the LOPD*

Faced by the current inconsistent rules regarding computation of terms, the regulations will establish a single formula for such computation, whatever the procedure of those contemplated in the LOPD is involved. For these purposes working days will be taken as the standard.

d) *Establishment of formalities required for evidencing compliance with the information obligation and obtaining consent. Specific regulation for data of minors*

Given the lack of precision in the Act in this regard, of particular relevance are the judgments of 24 January and 9 May 2003 of the Disputed Administrative Branch of the National Audience, with regard to *notices* to data subjects of their inclusion in the files, as well as the judgment of 30 June 2004 on *evidencing consent of data subjects to processing and transfer of their data.* The first two held in favour of two appeals of resolutions of the Agency ordering the archiving of proceedings, holding that notice to the data subject of his inclusion in the file had been proven. The National Audience on the contrary held that there was no such proof, arguing that "no legal or regulatory rule clearly requires that the communication sent to data subjects regarding inclusion of their personal data in the file be sent by certified mail with acknowledgment of receipt or by any other means giving documentary evidence of receipt. Nevertheless, since there are legal provisions that mandate such communication (articles 5.4 and 29.2 of Organic Act 15/1999) and characterize violation of this information obligation as a serious violation (article 44.3.1 of the Organic Act), it must be concluded that when the addressee denies having received notice the burden of proving the communication falls on the file controller."

The last of the cited judgments is to the same effect, holding that "...the individual or legal person attempting to obtain such consent must have the means necessary so that there is no doubt that consent has in fact been given, that is, that transfer of the personal data has received clear and conclusive consent."

The draft regulations scrupulously respect the definition of consent contained in the LOPD. Nevertheless, following the precedent of Royal Decree 424/2005 of 15 April 2005, they contemplate procedures that allow the processing controller to show that consent has been obtained using an auditable control of request for consent and a control of returned requests, because under the case law I have just cited it is the processing controller that has the burden of proof. Nevertheless, when there is any doubt as to whether consent has been obtained, the processing is not to be undertaken.

In addition, the draft establishes how consent may be revoked. Revocation is distinguished from the right of cancellation. Thus, the controller for revocation is not to impose additional requirements, such as those contemplated for the exercise of the rights of rectification and cancellation.

Regarding the information obligation, as a notable innovation the draft regulations also include specific regulation of the obligation of *information to minors.* Under the provisions that are established, such information must be expressed in language that is easily understood by minors. It must expressly indicate the possible consequences of processing of their personal data.

As regards the giving of consent, the draft contemplates that in the information sent to minors it must be expressly indicated, if applicable, that the consent of their parents or guardians will be required for processing.

e) *Detailed regulation of the concept of "processor" and requirements related to subcontracting of services*

Regarding the formal requirements for the existence of a *processor* under article 12 of the LOPD, AEPD opinions again have been of great importance. They were confirmed by the Disputed Administrative Branch of the National Audience in its judgment of 19 November 2003. Therein it holds that proof of entering into and the content of the contract can be shown only if it is in writing or in another form allowing verification of its content. Otherwise the processing of the data falls under article 6 of the LOPD.

It also is appropriate to mention the judgment of the Disputed Administrative Branch of 21 July 2004. It is clarifying regarding the same article 12 of the LOPD, as regards the processing of data on behalf of third parties and subcontracting. It also requires formal evidence of the contractual relationship existing between the controller and processor. Furthermore it clarifies the limits within which third parties must act, making it clear that the subcontracted companies must act subject to the provisions of the LOPD.

Regarding this matter it is appropriate to take the Agency's criteria into account. They were first expressed through *AEPD Instruction 1/2000 of 1 December*

2000 on rules regulating international movements of data, in particular its sixth rule, which contains the *particular rules for transfers the purpose of which is processing data on behalf of the file controller.*

This Instruction maintained the view that it is not possible to subcontract with another company unless it acts for and on behalf of the file controller.

Later, this criterion was expanded by recommendations prepared in this regard by the Agency. (We refer to the recommendations made regarding the Ex Officio Sector Inspection of INE in 2001.)

These recommendations, on the one hand, state the requirement that the *processor,* before providing the services, sign a contract with the contracting company containing and satisfying the requirements set forth in article 12 of the LOPD. But in addition, the file controller must establish the measures of a technical and organizational nature that must be adopted by processors to ensure security of the personal data and avoid their alteration or loss, or unauthorized processing thereof or access thereto. Also, depending on the characteristics of the information processed by the processor, based on kind and volume, and by reference to the greater or lesser need to ensure confidentiality and integrity thereof, the file controller is entitled to exercise control during the term of the contract to verify compliance with the established security measures and adopt appropriate corrective measures.

On these terms, once the services have been completed the media must be returned to the file controller or destroyed, or all files containing personal data must be erased by the processor. There must be evidence that these requirements have been satisfied. For this purpose the issuance of a certificate to be sent to the file controller may be considered to be a good practice.

In addition, if the processing controller wishes to replace a service provider with another one, the return of the data may be to the new processor, provided that there is an express provision in this regard and compliance with the principles contemplated in the LOPD is guaranteed. The intent is to facilitate the replacement and reduce the costs inherent therein.

Further, regarding the obligation to destroy the information, the draft regulations clarify that the processor may, with proper blockage, retain the data for so long as liability may derive from its relationship with the processing controller.

In addition, regarding subcontracting these recommendations indicate that if a services provider contemplates or enters into a *subcontracting* relationship that implies processing personal data, the requirements of data protection rules must be reflected in the contract. In addition to satisfying the requirements of referenced article 12, the contract either must expressly state that the services

contractor acts for or on behalf of the file or processing controller or, alternatively, must specify the following cumulative requirements:

— That the services to be subcontracted are expressly contemplated in the offer or the contract entered into between the file controller and the processor.
— That the specific details of the subcontracted services and the subcontracting company appear in the offer or in the contract.
— That the personal data processing by the subcontractor is in accordance with the instructions of the file controller.

f) *Regulation of the right of opposition*

As I have already stated, the right of opposition first appeared in the LOPD. It was not covered by the LORTAD. For this reason the pre-existing development regulations referred expressly and only to rights of access, rectification and cancellation. Nevertheless, although this circumstance did not result in any obstacle to full application, it did result in doubts regarding its effectiveness and the legal system applicable thereto. These initially were clarified by the Agency resolution of 22 October 2003, which recognized its full effectiveness and established procedures and terms for its exercise. Is also provided an interpretation of our legal system consistent with the requirements of community law. The draft regulations definitively clarify the applicable system.

They also describe the circumstances in which exercise of the right of opposition is allowed, following the structure of Section VII of Chapter II of the Community Directive, referring to the "data subject's right of opposition."

g) *Regulation of Security Measures*

As has already been indicated, the LOPD within its scope of application includes both automated and non-automated files and processing. Nevertheless, the current regulations of security measures applicable to files refer only to automated files, because they are contained in a Royal Decree (Royal Decree 994/1999 of the 11 June 1999) issued in development of the prior LORTAD.

Although this Royal Decree remains in effect, to the extent not contrary to the LOPD, it is clear that it is necessary to develop the security measures applicable to both kinds of files and processing, which will be done through the regulations that are being prepared.

As the most relevant innovations of the new text we would highlight the changes introduced in the categories of files that are subject to the various levels. Thus, in the medium level are included files that contain data regarding certain

social groups of special sensitivity, such as victims of sex crimes, and files containing data regarding telecommunications usage.

The regulations also deem it to be appropriate to include adequate access control as a medium level security measure. And at the high level the regulations include files containing communications localization data. In addition, excepted from this level are files and processing regarding ideology, union affiliation, religion and beliefs, and regarding health, the purpose of which is solely management of obligations by the one retaining the data.

We also considered the possibility of excepting data related to money transfers by employees to the entities of which the data subjects are associates or members. But based on comments of a labour organization, this exception may not be absolute, maintaining some specific high level security measures.

On a general basis, we also have included an obligation to notify the Agency of the dates of audits required for medium level files, including a statement as to whether the audit was internal or external.

Regarding security measures for non-automated files, the regulations address the existence of physical access control, guarantees of preservation, locating and querying information, a system for recording entry and departure of documents and procedures for control of copying or reproduction thereof. Measures are also established to prevent access to manipulation of the information during its transfer.

h) *Detailed regulation of international transfers*

The draft regulations clarify what is meant by international data transfers, to adjust the text to community rules. Thus, transmission of data is a transfer only if the destination is within the European Economic Area.

In addition, article 33.2 of the LOPD, regarding international movement of data, provides that "The adequacy of the protection level offered by the destination country will be evaluated by the Data Protection Agency based on all of the circumstances affecting the transfer or category of transfer of data. Taken into account in particular will be the nature of the data, the purpose and duration of processing contemplated, the country of origin and the country of final destination, the rules of law, general or by sector, in effect in the third country in question, the content of the reports of the Commission of the European Union, as well as the professional rules and security measures in effect in those countries."

As I commented earlier, the First Report of the European Commission on the application of Directive 95/46/EC, published on 15 May 2003, expressed certain

doubts regarding the binding nature of the *European Commission Decisions regarding Adequacy of Protection in third countries.* Nevertheless, despite the fact that the LOPD does not expressly so characterize them when it provides in its article 33.2 that "the reports of the Commission will be taken into account," the AEPD always has accorded them that character by application of the principle of the primacy of community law, and has ceased to require the prior authorization mandated by the LOPD after the effectiveness of all of them.

Nevertheless, the regulations developing the LOPD must clarify that this authorization of the Director of the Spanish Data Protection Agency will not be necessary to make an international data transfer when the importer is located within the territory of a State with respect to which the European Commission has declared the existence of an adequate level of protection. In this manner the binding nature of the Decisions of the Commission in this regard will be emphasized.

- *The regulations in addition will be a suitable instrument for handling regulation of certain* procedures not contemplated in the current rules. *Examples are the procedure for preparation and approval of the Model Codes contemplated in article 32 of the LOPD, the procedure for cancellation of registrations with the General Data Protection Register, and the procedure for preparation of Instructions.*

In addition, in line with the work undertaken within the European Data Protection Authorities Group (Article 29 Party) they could handle regulation of the *procedure for notification of files and processing* in accordance with the recommendations of that Party regarding *simplification* thereof. In this regard, the AEPD is working on significant simplification of the forms for notice to the General Data Protection Register to facilitate compliance with this obligation by file controllers, contributing to achieving standardization of personal data protection culture. As a result of intense work of the Agency it very recently, specifically last 12 July, presented the new "NOTA" telematic notice system. It allows giving notice of files using various kinds of forms, and results in notable simplification by comparison with those in effect to date. It will be complemented by the possibility of undertaking the entire notice process by telematic means, through implementation of instruments of electronic administration or electronic signature certificates.

- In addition, the regulations *will clarify certain questions that have raised doubts regarding implementation of Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such

data, as a result of the conclusions of the First Report of the European Commission on application of that directive, published on 15 May 2003, to which I have already referred.

In this report the European Commission states a series of doubts regarding interpretation that it has discovered regarding implementation of that directive in the various Member States.

On this point I would like to state that the Spanish Data Protection Agency, in its supervision of compliance of Spanish legislation regarding this matter, has always interpreted Spanish rules in a manner harmonized with community legislation, and has taken action to implement the recommendations made by the European Commission in that report.

Among the most important of these actions I would note the Agency initiatives to increase the *transparency* of its actions. Among these, it is particularly worth noting the amendment of article 37 of the LOPD, by Act 62/2003 of 30 December 2003 on tax, administrative and social order measures, further developed by Agency Instruction 1/2004 of 22 December 2004, which was published in the Spanish Official Gazette of 5 January 2005. It establishes the terms on the basis of which such publication must be made, regulating the form and terms applicable for that purpose.

Pursuant to these provisions, the Agency is required to publish its resolutions, provided that they relate to procedures commenced on or after 1 January 2004, or relate to the file of inspection actions initiated on or after that date.

The publication of such Agency resolutions now is a reality. It contributes very significantly to increasing the transparency of the actions of the Agency and results in a guarantee of legal certainty for those subject to the rules.

Companies, public authorities, the courts, citizens and, ultimately, all those who are within the scope of application of the LOPD now have direct access to this information. Therefore they can directly know the criteria used by the Agency in the exercise of its authority, since publication of the indicated resolutions is made on the Agency's website.

In addition, it must be noted that the publication of the resolutions is after removing the personal data referred to in article 3 a) of the LOPD. In no case do the resolutions contain data relating to the addresses of private organizations, individuals or professionals affected by the resolutions.

In addition, the Commission expressed doubts regarding the *application of article 5.5* of the LOPD, which were dispelled by various statements of the Agency in 2004, to the effect that the personal data processing controller is exempt from the obligation to inform the data subject when, not having collected the data from

the data subject, they are obtained by virtue of a transfer or processing expressly contemplated by law. This was based on article 11.2 of the referenced directive. The doubts arising from this article of the LOPD must be interpreted by reference to the provisions thereof.

Another question raised by the Commission relates to *implementation of art. 7.f) of the directive.* It allows processing of the data in question to satisfy a legitimate interest of the processing controller or the transferee, if not overridden by the right of the data subject.

The AEPD has had occasion to apply this rule in some of its resolutions and legal reports, related to the insurance and telecommunications sectors, as well as the exercise of the professional activity of solicitors and barristers.

The draft regulations incorporate these precedents, clarifying that processing and transfer of the data are permissible when they "have as their purpose the satisfaction of a legitimate interest of the processing controller or transferee covered by a rule with the rank of an Act or a rule of community law of direct application."

In any event, they apply the rule of balancing interests, by adding that the transfer and processing will be permissible "provided that the interest or fundamental rights and freedoms of the data subjects contemplated in Art. 1 of Organic Act 15/1999 do not prevail."

Finally, the draft regulations incorporate into Spanish legislation certain definitions from the directive that are omitted by the LOPD, such as "third party" and "destinee."

- In addition, the regulations could *include regulation of new matters* deriving from the activities of the European Union, in particular as regards international data transfers within large multinational companies.

In this regard it is interesting to note the recent adoption by the European Data Protection Authorities Group (the Directive 95/46/EC Article 29 Party) of a system that allows structuring international data transfers within the scope of operations of these kinds of companies, on the basis of the so-called *binding corporate rules.*

By means of these rules, groups of companies may, by preparing corporate rules that ensure compliance with national data protection laws, provide guarantees that allow them to obtain the corresponding authorization of the data transfers they make, always within the group itself.

The regulatory development of the LOPD would allow incorporation of new matters like this one I have referred to, establishing clear regulations in this regard facilitating application of this system in our national environment.

By way of summary, I believe it is absolutely necessary to have regulations *of the LOPD* that include a clear and detailed statement of purpose, remedying the already mentioned absence of a preamble in the Act. Regulations that, by approaching regulation of the subject matter on an overall basis, end the existing dispersement of rules, at the same time resulting in greater transparency contributing to dispel the doubts that have arisen regarding application of the current rules as a result of their varying hierarchical rank (Royal Decrees, Instructions of the AEPD). Regulations that cure certain deficiencies of the structure of the LOPD itself, and help dispel doubts that have arisen regarding interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In short, regulations that regulate the subject matter in a manner consistent with the reality that now exists and the level of technological development that has been achieved.

Finally, by way of conclusion, I believe that regulatory development of the LOPD is the suitable option for approaching the matters I have referred to. I believe the work that has been done, with such broad social participation, has been work of enormous importance, through which timely questions have been analyzed. As I have indicated, it is necessary to regulate them.

The experience obtained over the years since the LOPD came into effect, the doctrine, both case law and that produced by the Agency itself, as well as the evolution of society itself and of the state of the technologies, have been essential elements. Taking them into consideration and analyzing them in depth, as has been done, has contributed to improving the level of the work undertaken and the results achieved. I honestly believe they can be graded as being very good.

Let us be confident that after approval of this proposal, its application and future practice, we will see that we truly have achieved greater clarification of the rules governing this fundamental right, and that the Agency, with the effectiveness expected of it, will truly be capable of meeting the challenges facing us in the near future.

2

Regulatory Development of the LOPD

Antonio Troncoso
Director of the Madrid Region Data Protection Agency
Chaired Professor of Constitutional Law

The need for Regulations developing the LOPD: A first evaluation

The Spanish Data Protection Agency and the Ministry of Justice are jointly working to prepare draft regulations for development of Personal Data Protection Act 15/1999 of 13 December 1999 (the "LOPD"). These regulations must be approved by Royal Decree of the Council of Ministers. For this reason, although at the outset the initiative is that of the Spanish Data Protection Agency, thereafter the draft must be analyzed and defined by the Ministry of Justice. Complex administrative proceedings will apply: hearing arguments, particularly from the sectors involved; requesting the mandatory reports; agreeing on the text with the various ministerial departments and with the autonomous communities; and, finally submitting the draft regulations to the Council of Ministers for approval as a Royal Decree. It must be noted that the lengthy processing of the regulations is allowing intense debate, much broader than that drawn by the LOPD that these regulations develop. In any event, and above all, we must

recognize the effort of the Spanish Data Protection Agency in introducing this draft.[1]

Before considering why regulations developing the LOPD have been prepared, we must analyze what the willingness to approve them means in terms of political will. In this regard it must be noted that the willingness to use a Royal Decree to approve regulations that maintain the provisions of the LORTAD [Organic Automatic Data Processing Act] and the LOPD means that the government has discarded the possibility of amending the LOPD to amend certain concepts. Thus, the Grupo Parlamentario Socialista [Socialist Parliamentary Group] while it was in the opposition (during the most recent legislative session) had presented a Proposal, but not of an Act, so that consent could be given only expressly, to abolish the marketing census.[2] Therefore, approval by the government of a Royal Decree consolidating the criteria established in the LOPD makes the possibility of amending the Organic Act to achieve a text more protective of the fundamental right to personal data protection more remote. Again we see how much positions change from being in the opposition to having the responsibility of governing.[3] The Grupo Popular [Popular Group] and Izquierda Unida [United Left] (some of whose members now are in the Grupo Socialista) appealed the LORTAD before the Constitutional Court, but thereafter supported the same concepts they had challenged, promoting the LOPD. The Grupo Parlamentario Socialista sometimes questioned the LOPD while in the opposition, but now as the government does not support its reform. Rather they undertake its regulatory development. All of this gives us the opportunity to again insist that what is important in life is taking balanced positions, and that without doubt what is most centring is governing. The regulations, like the data protection laws at the time, in this area attempt to balance the various interests involved when one analyzes the requisite protection of personal data.

The refusal to amend the LOPD means that the regulations must satisfy other purposes, some of which (as we will see later) are beyond the scope of regulations

---

[1] It takes a lot to prepare regulations. It is simpler and more comfortable not to do so. I therefore wish to expressly praise the work of José Luis Piñar Mañas, whom history will remember as the director who promoted approval of such necessary regulations. I would also like to recognize the effort and sacrifice of all those who collaborated in their preparation, working overtime, in particular Jesús Rubí, Agustín Puente, María José Blanco and Álvaro Canales.

[2] Amendment of the LOPD was repeatedly proposed by the Information Technology and Freedom Commission.

[3] It is not wrong to change one's opinion when it is the result of a new way of seeing things after reflection. But it is always suspicious (at least by reason of lack of moderation) when the change in opinion coincides with changes in public responsibility.

by reason of the ranking of rules. The regulations are necessary to the extent that it is necessary to correct some of the defects of the LOPD. As we already have commented on another occasion,[4] this is an inappropriate legislative technique. Thus, the LOPD has no statement of purpose, for which reason we do not know the legislative intent, one of the criteria for interpretation to determine the meaning of legal rules.[5] In addition, the LOPD does not have a reasonable classification system, particularly regarding regulation of processing undertaken by the Public Administrations.[6] These difficulties result from the risky manner in which it was handled by Parliament. What originally was a proposed law to amend certain provisions of the LORTAD to adapt it to Directive 95/46/EC, on the basis of a draft prepared by the government, in the preparation of which the Spanish Data Protection Agency had a decisive role, was transformed into a complete new text of an Organic Personal Data Protection Act, prepared by the Constitutional Committee of the Parliament, which had the will and capacity to completely amend the LORTAD, which from any point of view was not necessary.[7] In any event, the preparation of a new text within the Parliament that had not received adequate study by the executive power (the various general technical secretariats and general regulatory suboffices of the various ministries, the state attorneys and the Council of State) resulted in the approval of the law not carefully drafted and with serious defects of a systemic nature.

The regulations also have been proposed as a manner of continuing implementation of data protection rules in accordance with the requirements of

---

[4] We here repeat what is stated in A. Troncoso Reigada, "La protección de datos personales. Reflexión crítica de la jurisprudencia constitucional", *Cuadernos de Derecho Público*, nos. 19-20, 2003, pages 231-334.

[5] The proposed law to amend the LORTAD did include a statement of purpose.

[6] For example, cases of data communication among Public Administrations without consent of the data subject are not covered by art. 11 but rather by art. 21. Art. 11 of the LOPD authorizes the transfer of personal data without consent of the data subject to parliamentary commissioners but not to the Parliament, for which reason it is necessary to seek justification in the Constitution itself and in the bylaws of the Parliament and the parliaments of the autonomous communities. See also the defective regulation of processing of health data in arts. 7.6 and 8. To this it logically is necessary to add the difficulties intrinsic in personal data protection, which is rather complicated. It is very technical legislation, with a vocabulary of its own. The result is that each of Directive 95/46/EC and the LORTAD and the LOPD contains a group of definitions covering what is meant by personal data, file, data processing, file controller, processing controller, data subject, dissociation procedure, processor, consent of the data subject, assignment or transfer and sources accessible to the public (art. 3 of the LOPD).

[7] The objectives of the proposed organic laws amending the LORTAD were basically protecting nonautomated personal data processing, as required by the directive, and including regulation of access to data on behalf of a third parties. Nevertheless, spokeswoman Bernarda Barrio proposed preparation of a new text, for which an extraparliamentary committee was formed. The text that emerged from this committee contained significant defects, which had to be amended on proposal of the Spanish Data Protection Agency through amendments in the Senate.

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. The Community Directive gives the Member States a small degree of discretion, although less than given by directives in the past. In 2003 the European Commission analyzed how Directive 95/46/EC had been implemented, discussing the real degree of implementation with each Member State. There was no intent to sanction. It was purely informational. The appropriate conclusions were drawn.[8] The regulations attempt to correct some of the errors in the LOPD in implementing the directive, which perhaps require an amendment of the Act.

The need for the regulations is also urged based on the significance and currency of personal data protection. Significance, because since Constitutional Court Judgment 292/2000 of 30 November 2000 the fundamental right of data protection is expressly recognized as an autonomous right independent of the right to privacy, which requires complete and adequate regulation. When the LOPD was approved we were not yet speaking of an autonomous right. Currency because the development of new information and communications technologies increasingly affects the lives of persons, both individual and social aspects. Let us not forget that it is information and communications technologies themselves that have accelerated the process of globalization and international data transfers. We are, therefore, faced by an expanding reality that demands an adequate regulatory framework.

The regulations also intend to give legal certainty and security to personal data protection. The current regulations on personal data protection are a development of the LORTAD, which was repealed by the LOPD. The legal requirement of regulatory development of the LOPD has not yet been satisfied. Rather the prior regulations remain in effect. Thus, the Third Transitory Provision of the LOPD ("Subsistence of pre-existing rules") indicates that "[u]ntil the provisions of the

---

[8] See L. CERVERA, "Informe de la Comisión Europea sobre el proceso de transposición de la directiva 95/46/CE por parte de España", *in voce*. In the judgment of the European Commission, there are some articles of the LOPD that differ from the Directive. Thus, the LOPD does not contain a definition of third parties or destinees; art. 7.f of the directive was not included in the LOPD. There is unfortunate drafting regarding the scope of application of the Act. The directive says one thing and the LOPD says another. This prevents the Act from being applied to data controllers domiciled in other member countries. Arts. 25 and 26 of the directive regarding international transfers have been inadequately implemented. Thus art. 25 says that no transfer will be made if the third country does not offer an adequate level of protection and that the Commission will supervise and determine which countries are adequate. By contrast, the LOPD does not indicate that the Commission will determine what country offers adequate protection. It rather says only that the opinion of the Commission will be taken into account.

first final provision of this Act are implemented, the existing regulatory rules will continue in effect, with their same rank, in particular Royal Decrees 428/1993 of 26 March 1993, 1332/1994 of 20 June 1994, and 994/1999 of 11 June 1999, to the extent not contrary to this Act." This absence of regulatory development has negative consequences. If the regulatory rules in effect are by way of development of the LORTAD and not of the LOPD, the regulatory rules cannot contain the innovations incorporated into the LOPD that amended the LORTAD. In addition, there are doubts regarding what regulatory rules are maintained in effect and what rules are repealed. The LOPD expressly states that Royal Decree 1332/1994 of 20 June 1994 remains in effect. It develops certain aspects of Organic Act 5/1992 of 29 October 1992 regulating the automated processing of personal data. Also still in effect is Royal Decree 428/1993 of 26 March 1993, approving the bylaws of the Data Protection Agency. It says nothing regarding Royal Decree 994/1999 of 11 June 1999, approving the Regulations of Security Measures for Automated Files containing Personal Data, or regarding the instructions of the Spanish Data Protection Agency. They must be understood to be in effect to the extent not contrary to the LOPD.[9]

What has been stated is particularly evident when we analyze protection of personal data in non-computerized files (the so-called structured manual files). The existing regulatory rules develop nothing with respect to nonautomated processing (it was impossible for them to do so since it is one of the innovations of the LOPD by comparison with the LORTAD). Nor is there consensus regarding application of the security rules for computerized files to manual files. Royal Decree 994/1999 of 11 June 1999 approving the Regulations of Security Measures for Automated Files that contain Personal Data contains both technical and organizational and functional measures. Nevertheless, legally it would be difficult to apply the measures contained in Regulations of Security Measures for Automated Files to manual flies. It would be even more difficult to interpret the technical measures (for example encryption) and apply them to manual files (guarded by a key). Therefore, the Regulations of Security Measures for Automated Files cannot

[9] Remaining in effect are Data Protection Agency Instruction 1/1995 of 1 March 1995 related to the provision of services regarding solvency and credit; Data Protection Agency Instruction 2/1995 of 4 May 1995 on measures to ensure privacy of personal data collected as a result of securing life insurance together with the grant of a mortgage or personal loan; Data Protection Agency Instruction 1/1996 of 1 March 1996 on automated files established for the purpose of controlling access to buildings; Data Protection Agency Instruction 2/1996 of 1 March 1996 on automated files established for the purpose of controlling access to casinos and bingo parlours; and Data Protection Agency Instruction 1/1998 of 19 January 1998 on exercise of rights of access, rectification and erasure.

be legally imposed. It is even less possible that violation of these measures could be sanctioned as a serious violation (art. 44.3.h) of the LOPD). As we have indicated on another occasion, a sanctioning resolution in this case "could violate the principle of legality in sanctioning administrative proceedings, which require that no one is to be punished for actions or omissions that at the time they occurred did not constitute administrative violations, in accordance with the legislation in effect at that time (art. 25.1 of the Spanish Constitution). It is one thing for the existence of the organizational security measures contemplated in the Regulations of Security Measures to also be *recommended* as regards computerized files. It is entirely a different matter to legally enforce them and use them to support a violation resolution when they are not observed. Let us not forget that in sanctioning administrative proceedings many of the principles of criminal law apply, including the principle of categorization as a crime (no crime without a law). In addition to the fact that analogy is prohibited in sanctioning administrative proceedings, the application of Regulations of Security Measures, expressly applying to *automated files*, to manual files is a clear case of overextended interpretation of the *in malam partem* kind, which is incompatible with the principle of administrative legality set forth in art. 25.1 of the Spanish Constitution. The best way to demand effectiveness of security rules for manual files after the LOPD is, simply stated, to approve Regulations of Security Measures for structured manual files by way of Royal Decree."[10]

Therefore, we do not have regulations that adequately develop the provisions of the LOPD, completing the legal system for protection of personal data, filling the legal vacuum, for example, as regards manual files. We therefore support general regulations developing the Act, avoiding partial regulations and the disbursement of rules that has occurred in the past.[11] The draft regulations, like the LOPD, attempt to establish general rules for data protection, but this Act also is full of exceptions, remitting many files to specific regulation. Nevertheless, like the LOPD, these regulations are in the nature of supplementary regulations for all files that are subject to more specific regulation.

The regulations developing the LOPD are also addressed to giving greater transparency to this matter. Data protection is a legal system that is characterized

---

[10] See A. Troncoso Reigada, "Introducción y Presentación" in the *Guía de protección de datos personales para Servicios Sanitarios Públicos*, Civitas-APDCM, Madrid, 2004, pages 52-58. The Data Protection Agency of the Community of Madrid has approved various Recommendations regarding security and custody of clinical histories and social histories on paper.

[11] Nevertheless, the regulations are only intended to develop the LOPD, not other related legislation such as the General Telecommunications Act, the Information Society Act and the Electronic Signature Act. This also has excessively delayed approval.

by its lack of transparency. It is designed only for those that have been initiated.[12] The regulations fail to provide clear criteria resolving doubts of those operating under them arising from daily experience as to how to respect the principles and rights with respect to some personal data processing. File controllers are entitled to a clear and coherent data protection legal system, with a set of rules that provide legal certainty for this area of social and administrative activity that is increasingly important and increasingly generates more complaints. These criteria come both from court precedents and the interpretations issued by the Spanish Data Protection Agency itself. Over recent years, both the Supreme Court and, in particular, the National Audience have developed case law regarding protection of personal data in the extensive litigation, in which they have had to apply the law and review resolutions of the Spanish Data Protection Agency. These criteria, which have been defining and interpreting the LOPD, must be contemplated by the draft regulations. Also, the Spanish Data Protection Agency has been developing its own doctrine, both in resolutions regarding inspection proceedings and in response to inquiries presented by file controllers and citizens. These criteria are found in the Spanish agency's various reports and on its website.[13] Nevertheless, there is no rule reflecting the most important elements of interpretation of the data protection legislation, systematically organizing them. This arrangement would provide legal certainty, with the file controller having clear parameters and a defined legal framework for the various kinds of personal data processing. The doctrine of the Spanish Data Protection Agency would cease to be accessible only those who have been initiated: those who are comfortable with the headings of the various reports or have become aware of the Agency's criteria by reason of having been involved in the proceedings or having made the inquiries (normally large law firms and consultants), so they would be accessible to all file controllers and all of those subject to the rules. The data protection legal system thus would gain in transparency. In fact, although the text ultimately may not be approved as regulations, this draft always will be a good instrument collecting the principal criteria for interpretation of personal data protection principles and rights.

Therefore, the opinion regarding the draft regulations cannot be other than positive. Of course the draft regulations, like any legal text, have debatable provisions, inevitable because they were drafted by a team of individuals.[14] Thus it can

---

[12] Which traditionally has been very good for law firms and consultants.

[13] Some criteria of the Agency are also found in instructions, which in fact are in the nature of regulations.

[14] The Data Protection Agency of the Community of Madrid prepared a report with comments on the draft regulations. This report is published in the *2005 Report of the APDCM (Agencia de Protección de Datos de la Comunidad de Madrid—Data Protection Agency of the Community of Madrid),* pages 131-154.

be stated that the draft presents problems of regulatory hierarchy. For one thing, there are provisions in the regulations that could imply development of fundamental rights, which is reserved to Acts.[15] The draft reproduces many provisions of the LOPD, which can be criticized from a legislative technique point of view. The original could be reduced by using simple references to the LOPD. In addition, the specific regulation of many kinds of procedures departs from the trend toward administrative simplification in search of general procedures.[16] At the same time, the draft contains internal procedures of the Spanish Agency which should not be approved in a Royal Decree, among other reasons because of the problem of locking within the hierarchy that this implies.

The regulations cannot solve everything, particularly the problems that derive from the LOPD itself. Thus, the regulations cannot resolve the problem of strict liability in this area. For example, a file controller who acts fairly, declares the file, complies with the information principle, implements the security measures, but faces a violation resolution by reason of failure to comply with the secrecy obligation of an employee that uses the data for another purpose. It is true that the differences between administrative and criminal proceedings, in addition to the greater seriousness of criminal conduct (many administrative violations are not criminal) lie in the fact that criminal proceedings require not only illegal conduct but also culpable conduct that is sanctionable (one must prove culpability, that is subjective liability), while in administrative proceedings there is strict liability. In any event, the Director of the Agency also can propose initiation of disciplinary proceedings, if applicable, as provided in the legislation regarding the disciplinary system for Public Administrations (art. 46.2 of the LOPD). Nevertheless, often this is not possible because the statute of limitations has expired.

---

[15] The first version of the regulations stated that their "purpose is development of the principles, rights, obligations and procedures guaranteeing the fundamental right of personal data protection, regulated by Organic Act 15/1999 of 13 December 1999". By contrast, the final version says that "[t]he purpose of these Regulations is development of Organic Personal Data Protection Act 15/1999 of 13 December 1999".

[16] The exception would be the procedures related to exercise of the sanctioning authority, specific regulation of which makes sense as it provides greater guarantees.

Analysis of the draft: principal innovations

The general provisions: special reference to the distinction between public and private files and regulation of lists of persons belonging to professional groups

The draft regulations are the first rules expressly speaking of the fundamental right of personal data protection. They did so in the already cited first version of art. 1, stating that the purpose of the regulations "is development of the principles, rights, obligations and procedures guaranteeing the fundamental right of personal data protection." The final version says that "[t]he purpose of these Regulations is development of Organic Personal Data Protection Act 15/1999 of 13 December 1999." But it maintains the reference to the fundamental data protection right in art. 85.4 and possibly in the preamble. Let us not forget that art. 1 of the LOPD, consistent with art. 18.4 of the Spanish Constitution, did not mention this right, since its purpose was "to guarantee and protect, as they relate to the processing of personal data, the public freedoms and fundamental rights of individuals, in particular their reputation and personal and family privacy." Characterization of the fundamental right of personal data protection as an autonomous right is a construction of the Constitutional Court.[17]

Of particular interest is the reference to the scope of application. Thus, the draft regulations indicate that "they will apply to all total or partial automated processing of personal data, as well as nonautomated processing of personal data that is or is to be included in a file." In this manner the regulations depart from their predecessors that developed the LORTAD to include nonautomated processing, specifically mentioning paper processing underlying input into a computer file. The LOPD limited its scope of application to individuals. But, as is well known, the case law of the Constitutional Court has recognized private legal persons as holding other rights under art. 18 of the Spanish Constitution such as reputation, privacy and image, although to a lesser extent than for individuals. Thus it is stated that "data processing related to legal persons is not subject to the provisions of these regulations, without prejudice to their application to the processing of data of individuals that provide their services or are related thereto." In this manner the regulations are open to the possibility of applying the legislation to files of legal persons containing data that are processed regarding persons such as legal

[17] We have referred to this question in A. Troncoso Reigada, "La protección de datos personales. Reflexión crítica de la jurisprudencia constitucional", op cit.

representatives or corporate officers, or the files of companies for which autonomous individuals work.

Of special interest is the exclusion of deceased individuals. Thus, the latest version of the draft states that "[t]he provisions of these regulations do not apply to data related to deceased individuals." The prior version was broader. It was "without prejudice to the provisions of law and, in particular, the rights recognized in Organic Act 1/1982 of 5 May 1982 on civil protection of the right to reputation, personal and family privacy and the individual's image." As is well known, Organic Act 1/1982 of 5 May 1982 did allow exercise by deceased individuals of the rights of reputation, privacy and image, through their family members or the Attorney General. It does not appear to be reasonable to recognize these rights to deceased individuals and deny them the fundamental right of personal data protection, which also is a right in the personal area that can also affect the scope of privacy (when the data are private). Much less can this be done through regulations, since the holding of a fundamental right is a matter reserved to the law, in this case reserved to an Organic Act. Let us not forget that regarding access to clinical history, Act 41/2002 gives family members the right to access the deceased's clinical history, unless it is shown that the deceased expressly prohibited it (art. 18.3 of the LOPD). In fact, to date the Spanish Agency has protected the right of family members to access the clinical history of the deceased.[18]

The draft regulations improve the regulation of files (they now refer to processing) to which the personal data protection system does not apply, defining it as excluded processing. Thus, it limits characterization of processing by individuals in the exercise of exclusively personal or domestic activities to such "processing regarding the activities as is undertaken within the framework of private or family life of individuals." Regarding processing for the investigation of terrorism and serious forms of organized crime, the regulations maintain the requirement that the file controller give prior notice to the Spanish Data Protection Agency of the general characteristics and purpose of the processing. Nevertheless, a kind of prior control is established upon request of a party that allows data subjects to gain greater information regarding the legality of the processing. Thus a provision is added for data subjects to request "that the Spanish Data Protection Agency verify the lawfulness of processing of their data in the circumstances contemplated in the preceding paragraph. The Spanish Data Protection Agency may have such assistance of the file controller as it may need for exercise of its

[18] In addition, the draft attempts to make the LOPD more consistent with the directive as regards the territorial scope of application.

verification authority. It will limit itself to responding to the data subject making the request regarding the fact of undertaking the verification itself, with no indication regarding the results."

Processing governed by specific provisions under the regulations falls in what are called "special cases." In one respect, the draft improves its legal description of such processing, making reference to the specific legislation. Processing of data contained in the personnel qualification reports referred to by the legislation regarding the personnel system of the armed forces refers to those regulated in art. 99 of Armed Forces Personnel System Act 17/1999 of 18 May 1999. Processing of images and sounds obtained through the use of video cameras by the security forces refers to those regulated by Organic Act 4/1997 of 4 August 1997 regulating the use of video cameras by the security forces in public places. By contrast, the processing of personal data deriving from the Civil Register and the Central Register of convicts and rebels generically refers to "the terms contemplated in the regulatory rules." The same is done regarding those regulated by electoral system legislation. In the second place, it is clearly established that processing governed by specific provisions is not excluded from the LOPD. Rather the specific regulations apply to it and the data protection legislation applies by way of supplement, being subject to supervision of the Spanish Data Protection Agency.[19] This is particularly important because often file controllers subject to specific legislation have felt that they are outside the scope of application of the LOPD and supervision of the Data Protection Agencies. Therefore, the draft regulations state that "the provisions of these regulations are applicable by way of supplement to [the special cases], and the Spanish Data Protection Agency with respect thereto has the jurisdiction contemplated in article 37.1 of Organic Act 15/1999 of 13 December 1999. And the draft contains a reminder that personal data processing for exclusively statistical purposes is covered by state or autonomous legislation regarding the public statistical function, "without prejudice to the authority attributed to the Spanish Data Protection Agency by article 37.1 m) of Organic Act 15/1999 of 13 December 1999, and its bylaws."

With the already mentioned intention of improving legal certainty, the regulations make an interesting effort in the definitions chapter. They add many more than are contained in the LOPD, some of them contained in the directive but not implemented in the LOPD. Thus, an "identifiable person" is defined as "any

[19] In this regard they also should mention the regional data protection agencies that have authority regarding statistical files of the Public Administrations and video surveillance files of the regional and local police.

person whose identity may be determined, directly or indirectly, using any information related to his physical, physiological, psychic, economic, cultural or social identity." It is further clarified that an individual "will not be deemed to be identifiable if such identification requires disproportionate amounts of time or activity." "Personal data" is better defined, so that it includes information regarding identified or identifiable individuals, that information being "numeric, alphabetic, graphic, photographic, acoustic or of any other kind." "Health data" is better defined, being classified as "data of a personal nature related to health," including (consistent with the pronouncements of the Council of Europe) "information concerning the past, present and future health, physical or mental, of an individual. In particular, data related to the health of an individual will be deemed to include data related to percentage of disability and genetic information." Also of interest is the definition of "nonautomated file," which of course did not appear in the current regulations. It is taken basically from the directive: "any set of personal data organized in a nonautomated form, structured in accordance with specific criteria regarding individuals, which allows access without disproportionate effort to their personal data, whether centralized, decentralized or dispersed on a functional or geographical basis."

We should specially note the definitions of publicly and privately owned files. The draft defines "publicly owned files" as "files controlled by constitutional agencies or agencies having constitutional relevance of the State or the Autonomous Institutions with functions similar thereto, Territorial Public Administrations, entities or agencies related to or dependent thereon having public legal personality and subject to administrative law, public universities and public corporations established pursuant to law, in the latter case provided that the files are strictly related to the exercise of the public authority given to them by their specific regulations." It defines "privately owned files" as "those controlled by entities subject to private law, in any case not involved in the exercise of public authority, including those files controlled by non-health foundations in the public sector, companies within the public business sector of the State, Autonomous Communities, Provinces and Municipalities, regardless of their share structure, and public corporations established pursuant to law to the extent the files are not strictly related to exercise of the public authority given to them by their specific regulations." The draft provides (it is the only possible interpretation) that public files are not only files of the Public Administration (constitutionally understood to be the Executive Power) but also files of other State authorities or constitutional or statutory agencies (or agencies having constitutional or statutory relevance). Thus public files, for example, include those of the national and regional parliaments and

commissioners thereof. It also must be noted that the latest draft specifically includes files of public universities as public files (although they may be subsumed in the category of public entities related to the Territorial Public Administrations).

The draft regulations restrict the scope of public files by requiring that, in order for a file created by a public entity to the public, it must not only have public legal personality but also must be subject to administrative law. Based on this criterion, business public entities (public legal persons that are governed by private law) including public entities (agencies, for example) that use not only public law but also private law may be excluded from public file characterization. The distinction between public and private files, in particular the establishment of restrictive criteria in the definition of public files, affects the legal system applicable to processing and the distribution of jurisdiction as between the State and the Autonomous Communities. For this reason it deserves more specific analysis. Thus, as we have noted on another occasion, public files are controlled by the Autonomous Agency and private files are controlled by the Spanish Agency. Public files are subject to a specific legal system as regards consent (art. 6 of the LOPD) and as regards transfers of data between Public Administrations for historical, statistical and scientific purposes (art. 11.2.e) of the LOPD), and for the exercise of similar jurisdiction or jurisdiction applicable to the same matters (art. 21.1 of the LOPD) not applicable to private files. Violation of a data protection rule regarding a public file results in a violation resolution (art. 45 of the LOPD) while for a private file it results in substantial economic fines (art. 46 of the LOPD). Public files are created by a provision of a general nature published in an Official Gazette (art. 20 of the LOPD), while private files are created by notice to the General Data Protection Register (art. 25 of the LOPD).

The definition of "public file" in the draft regulations openly contradicts the LOPD. Thus, there is no support in the LOPD for considering public files to include only files of entities having public legal personality that are subject to administrative law. Thus art. 20 of the LOPD, in the chapter regarding publicly owned files, provides that a general provision is one that creates, modifies or erases files of *the Public Administrations,* not requiring that they be subject to administrative law. The exception to the principle of consent of the data subject applies when the personal data are collected for the exercise of the "functions belonging to the Public Administrations within the scope of their competence," also without any reference to being subject to administrative law (art. 6.2 of the LOPD). Consent also is not necessary when the transfer is among Public Administrations and the purpose is later processing of the data for historical, statistical or scientific

purposes (art. 11.2.e) of the LOPD, with no reference to being subject to administrative law. The same may be said of the notice of data collected or prepared by the Public Administrations "for performance of their duties" that will not be transferred to other Public Administrations "for exercise of other jurisdiction or jurisdiction over other matters" and regarding transfer of personal data that a Public Administration obtains or prepares for another purpose" (art. 21 of the LOPD). The autonomous agencies are given jurisdiction over personal data files created or managed by the Autonomous Communities and by local authorities within their territorial scope (art. 41 of the LOPD), also without reference to being subject to administrative law or the exercise of public law authority. The same may be said of art. 46 of the LOPD when it regulates violations by the Public Administrations regarding the files they control (art. 46.1 of the LOPD). Therefore, the LOPD in none of its provisions requires that in order to speak of a Public Administration it must be fully subject to administrative law or the exercise of public authority, for which reason the draft to this extent violates the Act. The LOPD defines public files to be files of Public Administrations based on the concepts of "functions belonging to the Public Administrations," "within the scope of their jurisdiction," "for performance of their duties," "for the exercise of authority." That is, the determinative criterion is the existence of administrative jurisdiction.

In addition, the draft regulations openly contradict article 2.1 of Community of Madrid Personal Data Protection Act 8/2001 of 13 July 2001. It gives the autonomous agency control over files of all public entities, even if private law is applicable to them: "1. The Community of Madrid Data Protection Agency exercises its control functions regarding personal data files created or managed by the institutions of the Community of Madrid and by the bodies, agencies, public law entities and other public entities comprising its Public Administration, except for commercial companies referred to in article 2.2.c).1 of Act 1/1984 of 19 January 1984 regulating the Institutional Administration of the Community of Madrid."[20]

[20] The referenced article 2 of Act 1/1984 of 19 January 1984 establishes the agencies and entities that constitute the institutional administration of the Community of Madrid. It expressly provides: 1. The institutional administration of the Community of Madrid will be created, being subject to the provisions of this Act: a) The Autonomous Agencies. b) The Management Bodies without legal personality separate from the Community and, if applicable, the Autonomous Agencies. c) The Public Companies. 2. a) The Autonomous Agencies are the public law entities created by the Assembly Act, having legal personality and their own assets, separate from those of the Community, which as a part of the decentralization system are specifically made responsible for: the organization and administration of any public service and the funds assigned thereto; the performance of economic activities serving various purposes; and the administration of certain Community assets, whether owned by them or in the public domain. b) The Management Bodies without legal personality separate from the Community and, if applicable, the Autonomous Agencies, are those created by decree of the Council of Governance to directly provide certain public services, with

Therefore, the public law entities having their own legal personalities that, by reason of their activities, and by law, must adjust their activities to the private law system are within the jurisdiction of the Community of Madrid Data Protection Agency." Act 8/2001 of 13 July 2001 considers these files to be public, since it does not give the autonomous agency authority to impose economic sanctions. It would make no sense for them to be within the jurisdiction of the autonomous agency but subject to the legal system for private files. Under Act 8/2001 of 13 July 2001 the only files considered to be private and therefore not within the jurisdiction of the Community of Madrid Data Protection Agency would be those of public companies having the legal form of corporations, majority owned, directly or indirectly, by the Community of Madrid. Act 8/2001 only distinguishes on the basis of the existence of public law authority in the case of public law corporations. In order for files of public law corporations to be characterized as public files, it is not sufficient that they be used in the exercise of an administrative activity. Rather they must be "strictly related to the exercise of public law authority." This is because these corporations are of a mixed nature including administration and association with private persons. For this reason, their public or private nature depends on the nature of their activity. Although the purpose of Act 8/2001 is to give jurisdiction to the Autonomous Agency, and not to define public files, the reality is that the division of jurisdiction between the Spanish Agency and the Autonomous Agency was done on the basis of the differentiation between public files and private files found in the LOPD. It was so stated in the Report of the Spanish Agency in this regard.[21] Therefore, this reference in the regulations to the definition of public and private files could be null as it is contrary to Act 8/2001. It is clear that the draft regulations cannot affect jurisdiction defined by Parliament and cannot reduce the jurisdiction of the Autonomous Agencies. The problem now lies in the fact that the draft regulations affect the legal system for files.

What is behind the distinction between public files and private files is the concept of Public Administration, since public files are those owned by the Public Administrations. This is behind all of the problems of the Administration in the

---

their funding set forth in the Community Budget and, if applicable, in the budgets of the Autonomous Agencies, with the appropriate specification of credits. c) The Public Companies are: 1) The Corporations majority owned, directly or indirectly, by the Community or its Autonomous Agencies, unless under the Assembly Act a lesser ownership interest is expressly authorized. *2) The public law entities with their own legal personality that by reason of the nature of their activities and by law must adjust their activities to the private legal system.*

[21] We refer to the Report of 21 May 2001 of the Spanish Data Protection Agency on the draft Community of Madrid Personal Data Protection Act.

formal and substantive senses, regarding the reach of administrative action.[22] The restrictive criterion adopted by the draft regulations comes from Act 30/1992 of 26 November 1992, on the Legal System for Public Administrations and Common Administrative Procedure, which within its scope of application includes not all publicly entities with their own legal personality, but only when they exercise public authority (art. 2). Nevertheless, the purpose of this provision is to determine the scope of application of Act 30/1992 of 26 November 1992, not to define Public Administration. It is self-evident that this Act does not apply to public entities that choose to be governed by private law. But this does not mean that they are not public entities and parts of the Public Administration. Therefore, in our view, all files of the Public Administrations, that is of public legal persons, must be characterized as public files, without requiring that their activities be fully subject to administrative law, and without requiring that they exercise public law authority. The only exception is public law corporations. In order for their files to be characterized as public files, it is not sufficient that they be used in the exercise of an administrative activity. Rather they must be "strictly related to the exercise of public law authority."

The distinction between public and private files is of particular importance in the health area, in particular regarding the legal form adopted by the new public hospitals in the Community of Madrid. The Administration is responsible for defining the form of and legal system applicable to the health service. For this purpose it has discretionary authority,[23] but this definition affects the scope of personal data protection, particularly as regards treatment of the files as public or private. Under the current legal system for data protection, indirect management of the new hospitals, through various contractual techniques (concession, agreement), that make private persons responsible for providing hospital services, results in private files. Direct centralized management of the new hospitals would result in public files. The problem lies in decentralized direct management. Under Act 8/2001, the choice of a private legal form (a commercial company) to manage health would result in private files, while the choice of a public legal form (a public entity), even if subject to private law, would result in public files.[24] The

---

[22] We already have given our opinion regarding this question in A. Troncoso Reigada, *Privatización, empresa pública y Constitución* and "Dogmática administrativa y derecho constitucional: el caso del servicio público", *REDC* no. 57, 1999, pages 87-164.

[23] See L. Parejo, F. Lobo and M. Vaquer, *La organización de los servicios públicos sanitarios* (coord), Marcial Pons, Madrid, 2001, in particular pages 11-46 and 71-98.

[24] There is particular complexity regarding public health foundations regulated by Royal Decree Law 10/1996 of 17 June 1996, on new ways of managing illness, Act 15/1997 of 25 April 1997, on new ways of managing the National Health System, Royal Decree 29/2000 of 14 January 2000, approving the developing

latter would contradict the provisions of the draft regulations which would consider the latter to be private files. Nevertheless this distinction may still be criticized because the material activity is the same, public health assistance, regardless of whether it is provided by an Administration, a public entity, a commercial company with public participation or a private company, the latter on behalf of the Administration.[25] In addition, many health management files, for example electronic clinical histories, do not allow private companies providing a public service to make decisions regarding use of the file. Without doubt, the use of the legal form of the person when distinguishing between public and private files presents an advantage of legal certainty.

There are other definitions in the draft regulations covering concepts that were already clear, with respect to which there was no doubt. But they have a teaching function for those approaching this subject matter for the first time and reading the regulations.[26] Thus, there is nothing new in the definition of a third party as "an individual or legal person, public or private, or an administrative agency other than the data subject, the processing controller, the file controller, the processor and the persons authorized to process the data under the direct authority of the processing controller or processor."[27] The same may be said of the definition of blockage: "the identification and withholding of personal data to prevent its processing except by Public Administrations, judges and courts to attend to possible liability arising from processing, and only until expiration of the statute of limitations for such liability." In the final version it is clarified that the blockage may result from compliance with the obligation imposed on

---

regulations and art. 111 of Act 50/1998 of 30 December 1998, on Tax, Administrative and Social Order Measures. This defines Public Health Foundations as "public agencies under the National Health Institute" (art. 2). In fact, art. 3.2 of the Decree of 29 January 2004 establishing the organic structure of the Ministry of Health provides that "[t]he institutional administration under the Ministry of Health and Consumption is comprised of the following public entities and autonomous agencies: Ente Público Fundación Hospital de Alcorcón". As under the criterion already explained they are public law persons, their files would be considered to be public files. Nevertheless, the Spanish Agency (Report 66/2003 published on its website) considers these files to be private because these foundations do not exercise public law authority, by virtue of art. 46.l.a) of Foundations Act 50/1992. Regarding this legal form, see M. VAQUER, *Fundaciones públicas y fundaciones en mano pública.* La reforma de los servicios públicos sanitarios, Marcial Pons, 1999, and his contribution to the work cited above.

[25] This is why Act 5/2002 of 19 April 2002, creating the Catalonian Data Protection Agency, and the Statute of Catalonia give the Catalonian Agency jurisdiction over private entities that provide public services, although the legal system applicable thereto is not clear.

[26] We will not now analyze the definitions related to security measures, which are deserving of specific study.

[27] The provision in the case of entities without legal personality that act in trade as distinct persons is of interest. The person or persons comprising them are considered to be third parties.

the controller to cancel data when they cease to be necessary for or pertinent to the purpose for which they were collected or for exercise of the right of cancellation. There also is nothing new in the definition of erasure.[28] The same is true of the definition of international data transfer.[29] Nevertheless, it does not make much sense for the draft regulations to repeat definitions already found in the LOPD. This is the case of the definitions of consent of the data subject,[30] file, transfer or communication of data[31] and data processing.[32] Of no particular interest are the definitions of file controller,[33] anonymous data or anonymity procedure,[34] destinee or transferee,[35] processor (which incorporates the content of art. 12 of the LOPD),[36] personal data exporter[37] and personal data importer.[38]

The general provisions of the draft regulations also cover sources accessible to the public, repeating the definition and list in art. 3.j) of the LOPD. It is notable

---

[28] Erasure is "the physical elimination of the blocked personal data, after expiration of the statute of limitations for any possible liability arising from processing, during which period they remain blocked".

[29] "Data processing that results in transfer thereof outside of the European Economic Area, whether it is an assignment or communication of data or has as its purpose the processing of data on behalf of the file controller established in Spanish territory".

[30] It is not required that the consent be express (it could not be so required by regulation).

[31] Only a small change, from "any disclosure" to "data processing that results in its disclosure".

[32] Thus, only two items are added to the definition of data processing that appears in the Act: "any technical operation or procedure, whether or not automated, that implies collection, recording, retention, elaboration, modification, *querying, use,* blockage or cancellation, as well as data transfers resulting from communications, inquiries, interconnections and transfers".

[33] Where the LOPD defined it as the "individual or legal person, public or private, or administrative agency, that decides regarding the purpose, content and use of the processing", the draft adds "even if it does not physically do so". The clarification in the case of entities without legal personality that act in trade as distinct persons is of interest. The person or persons comprising them are considered to be processing controllers.

[34] Anonymous data are "data that do not allow identification of a data subject" and anonymous processing is "all processing of personal data that allows anonymous data to be obtained".

[35] "The individual or legal person, public or private, or administrative agency, to which data are disclosed". Of more interest is the provision to the effect that "in the case of entities without legal personality that act in trade as distinct persons, the person or persons comprising them are considered to be the destinee".

[36] "The individual or legal person, public or private, or administrative agency that, itself or together with others, processes personal data on behalf of the processing controller or the file controller, as a result of the existence of a legal relationship that binds it therewith and specifies the scope of its actions in the provision of the services. In the case of entities without legal personality that act in trade as distinct persons, the person or persons comprising them are considered to be the processor".

[37] "The individual or legal person, public or private, or administrative agency located in Spanish territory that is the processing controller of personal data that are internationally transferred to a third country".

[38] "An individual or legal person, public or private, or administrative agency that receives data in the event of an international transfer thereof to a third country, whether it is the processing controller, processor or a third party".

that the marketing census contemplated in the LOPD is not abolished. Telephone books are now classified as "electronic communications services guides." Regarding lists of persons belonging to professional groups it is specified that the address datum is the business address. Data that may be included in such lists are the complete postal address, telephone number, fax number and e-mail address. The draft regulations clarify that as an indication of membership in a professional group (in the case of professional associations) the list may include the membership number, date of joining and status of exercise of the profession.

In this manner, the draft regulations open debate regarding processing of data of those not exercising the profession appearing in the membership list and telephone list. The public file of the members includes both those who are in practice and those who are not. Those not in practice are in the membership file to the extent that they may become practicing professionals. The datum regarding not being in practice is information related to supervision of exercise of the professional activity, which justifies its inclusion in the membership file. Consent of the data subject is not necessary because the professional association satisfies the administrative function of organization of the profession. That is, although membership is voluntary for one not in practice, registration as a member is an administrative function and denial of such registration is appealable to disputed administrative jurisdiction.[39]

The lists of persons belonging to professional groups, which are sources accessible to the public, are a different matter. The membership file is not a source accessible to the public and is not the same as this list. By publishing the list the professional association also fulfils a professional organization function, avoiding the entry of unqualified people into the profession, performing a function of public law. Those in practice must appear on this list. No consent of the data subject is required, because this is an administrative function. The member may exercise only the right of opposition.[40] Based on the draft regulations, this list may also publish the data of those not in practice. This publication also has an administrative function, related to supervision of the exercise (or lack of exercise) of the profession. What we have is public law authority. For this reason the non-practicing members have their data published without their consent, without prejudice

[39] Those not in practice are only subject to a special relationship with the professional association regarding potential exercise of the profession. The other relationships of those not in practice with the association are relationships among private parties in exercise of the right of association.

[40] Because this list is a source accessible to the public, the data subject has the right to indicate that his data are not to be used for commercial purposes.

to the right of opposition.[41] In any event this position appears to have been contemplated by Parliament, when it stated that "indication of membership in the group" is a part of the list. One not in practice clearly belongs to the professional group. In addition, the fact that the draft regulations clarify that among indicators of belonging to the group is the "status of exercise of the profession" implies that there are various statuses, and that all of them would appear in what would be called a list of "persons belonging to professional groups" and not a list of "persons exercising the professional activity." This concept maintains the unity of the legal system for professional lists and their treatment as public files.

Professional lists may mandatorily contain only the data included in art. 3.j of the LOPD. Any other information (hours open) requires consent of the data subject. As we have indicated, the draft regulations developing art. 3.j) include the doctrine already prepared by the Spanish Agency. They state that as a part of the data regarding membership in the group one may include the membership number, the date of joining and the status of exercise of the profession.[42] To clarify something else, one might even indicate that the association is to determine whether, in the list, it will provide this additional information regarding group membership. If the association so decides because it believes it is necessary in order for it to accomplish professional organization of the activity, consent of the data subject would not be necessary, but rather the right to exercise opposition.

Data protection principles

There are some provisions regarding regulation of the principle of quality of data, already implicit in art. 4 of the LOPD, in an attempt to better describe the content of that principle, but without specific practical consequences. This part of the regulations can be broken down into four parts, one regarding collection of data, another related to the life cycle of the file, and another regarding cancellation or retention of the information.

Thus, for example, it is stated that "personal data must be processed fairly and lawfully." This already has been stated in the European regulations and in the case law, which has repeatedly affirmed the principle of fairness and lawfulness. In

---

[41] It is true that some data in the list, such as the address, are particularly related to exercise of the profession, and not to its non-exercise. To soften this position, the right of opposition could be granted.

[42] Some doctors have opposed publication of the membership number in the professional list, fearing that drug addicts would find it easier to falsify prescriptions. Nevertheless, the Medical Association has not accepted such oppositions.

addition, two articles provide that personal data may only be collected for specific, explicit and lawful purposes of the processing controller, and that the data processed must be adequate, pertinent and not excessive by reference to the specific, explicit and lawful purposes for which they were obtained. This highlights the importance of lawfulness of the processing. This is particularly important in the administrative area. No agency may collect data if the purpose is not within its administrative jurisdiction.

In the second place, the draft does contain an important provision regarding the required accuracy and currency of the data, so that it will truly reflect the current situation of the data subject. Thus, the latest version of the regulations (not prior versions) provides that "[i]f the data are collected directly from the data subject, the data provided by the data subject will be deemed to be accurate." In addition, the provisions of the LOPD are clarified, with a reminder that if personal data subject to processing are inaccurate, in whole or in part, or incomplete, they must be cancelled or *also rectified* within a term of 10 days after learning of the inaccuracy. If these data have already been transferred, there is an added obligation of the file controller to notify the transferee of the rectification or cancellation within a term of 10 working days, provided that the transferee is known. Within a term of 10 working days after receipt of the notice, the transferee processing the data must rectify and cancel pursuant to the notice. This updating of the personal data does not require notice to the data subject.

In the third place, the regulations contain certain cases for retention of information despite the fact that it has ceased to be necessary or pertinent for the purpose for which it was collected. Thus, it is provided that data may be retained "for the period during which any kind of liability may be enforced, deriving from a legal relationship or obligation, or obligation to perform a contract, or obligation to apply precontract measures requested by the data subject." This retention is different from blockage, which is limited to the reservation of data to prevent their processing except by Public Administrations or the courts. In any event, we believe the two cases are similar, since retention to meet legal obligations prevents any other processing of the data for the principal purpose.

As is well known, art. 4 of the LOPD provided that, although data may not be used for purposes incompatible with those for which they were collected, processing personal data for historical, statistical or scientific purposes is not deemed to be incompatible. To determine what statistical purposes are, state and autonomous legislation applies, as do the provisions developing them. The draft expressly cites (the LOPD did not do so) Public Statistical Function Act 12/1989 of

9 May 1989, Spanish Historical Patrimony Act 16/1985 of 25 June 1985, and Act 13/1986 of 14 April 1986 on Promotion and General Coordination of Scientific and Technical Research. The draft regulations add a new possibility of exception to cancellation of data. The Spanish Data Protection Agency and the agencies of the Autonomous Communities may agree, upon application of the processing controller and pursuant to a specific procedure, on full retention of certain data based on their historical, statistical or scientific value.[43]

The draft regulations are particularly ambitious as regards consent and the information obligation. It is to be noted that consent is regulated in a section covering lawfulness of data processing. In addition, it is regulated jointly with lawfulness of data processing and transfers. This seems to us to be particularly wise, but it has been criticized by the Ministry. Thus, it is stated that the principal circumstance legitimizing data processing or transfer is consent.

Nevertheless, following the sense of art. 6.2 of the LOPD other circumstances justifying processing or assignment without consent of the data subject are listed.

In the first place, processing or transfer without consent is lawful if it is contemplated by law. The draft regulations expand on this by recalling that this is also possible under a community law of direct application. In addition, it is not necessary that the law or rule of community law allow the processing or transfer. Rather the purpose of the processing or transfer must be satisfaction of a lawful interest of the processing controller or transferee, covered by a rule having the rank of an Act or a rule of community law of direct application, provided that the interests or fundamental rights and freedoms of the data subjects contemplated in article 1 of Organic Act 15/1999 of 13 December 1999 do not prevail. It also is provided that processing or assignment without consent is lawful when it is necessary for satisfaction of an obligation of the processing controller that is contemplated in a rule with the rank of an Act or a rule of community law of direct application. What is most important is that the draft regulations do not require a rule that contemplates the processing or transfer, but rather a rule that recognizes a legitimate interest that requires the processing or transfer of the information. This is the most appropriate criterion for balancing the fundamental rights, balancing the interests and respecting the principle of proportionality. The fundamental right to data protection and consent of the data subject to the processing or transfer is also limited by other fundamental rights and other legal

[43] The draft regulations could have addressed the problems regarding the term for retention of clinical histories, fixed by Act 41/2002 at a minimum of five years, but increased by autonomous legislation (an unlimited term in the case of Galicia and 20 years in the case of Catalonia).

interests recognized by law, although they do not expressly contemplate transfer of the information.[44]

In the second place, data processing by and data transfers to the Public Administrations are analyzed. Art. 6.2 of the LOPD excludes the requirement of consent when data are collected for the exercise of functions belonging to the Public Administrations within the scope of their jurisdiction. The draft regulations say "by a Public Administration within the scope of its jurisdiction." The narrower definition of this concept excludes, for example, data collected by private entities that perform administrative functions. Consent also is not required for a transfer when the destinee is a Public Administration and the data are processed by it exclusively for historical, statistical or scientific purposes (art. 11.2.c). The draft regulations are very advanced regarding transfer of data among Public Administrations. Art. 21.1 the LOPD, based on Constitutional Court Judgment 292/2000 of 30 November 2000, allows the transfer of data among Public Administrations for the exercise of similar jurisdiction or regarding the same matters. Nevertheless, the draft regulations state only that "the personal data are transferred to a Public Administration within the scope of the jurisdiction given to it by a rule with the rank of an Act or a rule of community law of direct application." This provision is nothing more than a repeat of the lack of required consent when there is legal authorization for the transfer, whether or not a Public Administration is the destinee. Art. 21.1 of the LOPD allows transfer of data among Public Administrations without such legal authorization. Thus, this possibility is not contemplated in the regulations. Regarding this position, administrative jurisdiction is not always contemplated in a rule with the rank of an Act. Nevertheless, an interpretation that stated that all work of the Public Administrations is legally authorized would allow the transfer of data among Public Administrations for different purposes, something that initially is incompatible with the literal sense of art. 21.1 of the LOPD.[45]

In the third place, processing or transfer of data included in sources accessible to the public is contemplated, when necessary to satisfy the legitimate interest

---

[44] This is the criterion that has been followed by the Community of Madrid Data Protection Agency in Recommendation 1/2006 regarding transfer of data from the government to unions. It legitimizes not only transfers contemplated by law, but also those necessary to guarantee the fundamental right to union freedom, as regards the functions of employment supervision and control. For greater detail see A. Troncoso Reigada, "Libertad sindical, libertad de empresa y autodeterminación informativa de los trabajadores", in A. Farriols, *La protección de datos de carácter personal en los centros de trabajo*, Ed. Cinca-Fundación Largo Caballero-CLI, Madrid, 2006, pages 103-138.

[45] An argument for greater flexibility in transfers of data among Public Administrations may be seen in A. Troncoso Reigada, "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", *Cuadernos de Derecho Público* 19-20, 2003, pages 231-334.

pursued by the file controller or by the third party to whom the data are transferred, provided that the fundamental rights and liberties of the data subject are not violated. Nevertheless, the transfer of data contained in sources accessible to the public by the Public Administrations may not be to private files, except with the consent of the data subject or when otherwise provided by law. The draft regulations here combine the provisions of arts. 6.2, 11.2.b) and 21.3 of the LOPD. The only thing added is the requirement that "[t]he data processed or transferred under this section must be only the data contained in sources accessible to the public, without prejudice to the cases in which the law authorizes the data subject to state his wish not to receive advertising," a provision contained in art. 28.2 of the LOPD).

In the fourth place, the draft regulations contemplate that the data processing may relate to the parties to a contract or precontract, to a business, employment or administrative relationship, and be necessary for appropriate maintenance, development (this is an innovation that was added to the concept of maintenance) or performance thereof. This provision is a reproduction of art. 6.2 of the LOPD. The draft adds that the legal relationship is between the data subject and the processing controller (which is obvious) and the relationship must be freely accepted by the data subject (which is a very interesting clarification). In any event, the draft also adds that the processing will only be lawful when limited to the legal relationship underlying it.

In the fifth place, a provision of art. 11.2.c) of the LOPD is rewritten. It allows transfer of data of a data subject when necessary for development, performance and supervision of a legal relationship, freely and lawfully accepted by it. In this case the transfer will only be lawful to the extent limited to the purpose underlying it.

In the sixth place, the draft regulations repeat the provision of art. 11.2.d) of the LOPD that allows transfer to the Public Defender, the Attorney General, judges or courts or the National Audit Office or the autonomous institutions with functions similar to those of the Public Defender or the National Audit Office, made within the scope of the authority the law expressly attributes to them.[46] The opportunity has not been taken to provide for transfer of data to the Parliament and the Autonomous Parliaments as would be deduced from the Constitution and the parliamentary statutes and regulations.

The draft regulations also cover the problems of specially protected data, in a provision called "authorization of processing of specially protected data." First of all, the draft clarifies that the exceptions to consent for processing and transfer

[46] It is better drafted since the LOPD only provided for exercise of the functions attributed to state agencies. In the case of the autonomous communities it had to be deduced.

established in the LOPD and in the regulations will not apply to processing or transfer of personal data revealing the ideology, union affiliation, religion and beliefs of data subjects, nor those related to their racial origin or sex life, which will be governed by the provisions of this article. This provision did not expressly appear in the LOPD and is very clarifying. Of special interest is the statement that "when the consent referred to in the following paragraph is obtained with respect to this data, the data subject will be advised of his right to withhold it." It is notable that the regulations for these purposes give the same treatment to data regarding ideology, union affiliation, religion and beliefs as they do to data regarding racial origin or sex life, whereas the constitutional (art. 16.2) and legal (art. 7.1 of the LOPD) prohibitions refer only to the former. Regarding personal data revealing ideology, union affiliation, religion and beliefs, the legal provision (art. 7.2 of the LOPD) is repeated, to the effect that such data may be processed or transferred with prior written consent of the data subjects. Excepted from the provisions of the preceding paragraph is processing undertaken by political parties, unions, churches, denominations or religious communities, and non-profit associations, foundations and other entities, the purpose of which is political, philosophical, religious or of a union nature, regarding the data related to their associates or members. Nevertheless, the data may not be transferred to third parties without the prior, express and written consent of the data subject. The latter point improves on the drafting of the LOPD, which speaks of prior consent, although it may be indirectly deduced that it must be express and written. Regarding personal data referring to racial origin or sex life, they only may be collected, processed and transferred when, for reasons of general interest, it is so provided by law or the data subject expressly consents, repeating the legal provision in art. 7.4 of the LOPD without mentioning health data.

The processing of health data is separately treated by the draft regulations, in the section called "authorization for processing of specially protected data related to health." As with respect to other specially protected data, the draft clarifies that the exceptions to consent to processing and transfer established in the LOPD and the regulations will not apply to processing or transfer of data related to health. Processing or transfer of personal data referring to the health of data subjects may only be undertaken, repeating the provisions of art. 7.3 of the LOPD, with prior consent of the data subject or when, for reasons of general interest, it is so provided by law.[47] The only thing added by the draft is that it also may be so provided

[47] There is a debate regarding whether transfer of health data is contemplated in arts. 7 and 8 of the LOPD or, on the contrary, we must remit to art. 11 of the LOPD. The Spanish Agency in its reports regarding transfer of health data never cites art. 11 of the LOPD. We believe that this article is also applicable

by a rule of community law of direct application, of course also for reasons of general interest. Nevertheless, the draft regulations themselves echo the legal provisions for processing health data without consent of the data subject, which serve as legal authorization. One (also contemplated in art. 8 of the LOPD) provides that "[i]n any event, public and private health facilities and health professionals may process the personal data related to the health of persons who seek their assistance or must be treated by them, on the terms contemplated in the state and autonomous health legislation," citing one of the most specific health laws that also has been recently approved: Act 41/2002 of 14 November 2002, the basic law governing the autonomy of patients and rights and obligations regarding clinical information and documentation. Another (contemplated in art. 7.6 of the LOPD), identified as "common provisions regarding processing of any specially protected data," is unique in that it not only allows processing of health data but rather all specially protected data. Thus, it is provided that specially protected data of data subjects may be processed when necessary for medical prevention or diagnosis, providing health assistance or medical treatments or management of health services, and the processing is performed by a health professional subject to professional secrecy or another person also subject to an equivalent secrecy obligation.[48] Specially protected data may also be processed when necessary to safeguard the vital interests of the data subject or another person, if the data subject is physically or legally incapable of giving consent (art. 7.6, second paragraph). Finally, the draft regulations repeat the authorization in art. 11.2.f) of the LOPD that allows transfer of data when necessary to perform epidemiological studies, on the terms established in the applicable state or autonomous legislation. It is notable that the draft omits another case contemplated in the same article, that is when the transfer of personal health data is urgently needed. In any event, this omission is not serious, because there is abundant legal coverage for processing and transfer of specially protected data for purposes of welfare.[49]

---

to specially protected data, and in addition expressly contemplates assignment in cases of urgency or for epidemiological studies. The underlying problem is whether it is possible to apply the provisions of art. 21 of the LOPD to transfer of specially protected data among Public Administrations, in this case the Health Administrations. We believe that art. 7 of the LOPD refers principally to consent to processing as an exception as regards art. 6 of the LOPD, while arts. 11 and 21 of the LOPD allow transfer, also applicable to specially protected data. Art. 8 of the LOPD would apply to both processing and transfer.

[48] The draft regulations could have taken advantage of the opportunity to resolve the problem of access by social workers to clinical history data in the social and health fields.

[49] The draft, under the heading "authorization for processing data regarding commission of violations", transcribes art. 7.5 of the LOPD which provides that "[t]he personal data related to commission of criminal or administrative violations may only be included in files of the competent Public Administrations in the circumstances contemplated in the respective regulatory rules".

The draft regulations regulate the criteria for obtaining consent. As a general principle they indicate that the processing controller must obtain consent of the data subject to process his personal data, except in the exceptional circumstances we have discussed above. Art. 3.h) of the LOPD indicates that consent of the data subject is any free, unequivocal, specific and informed expression of will, by means of which the data subject consents to the processing of personal data affecting him. The LOPD requires that the consent be specific and informed. This means that the person must consent to the processing of his data after having been informed of the specific purpose for which his data are collected. Therefore, the draft regulations indicate that "the request for consent must refer to a specific processing or a series of processing, stating the purpose for which they are collected and the other conditions affecting the processing or series of processing." This is applicable to both consent to processing and consent to transfer. Art. 11.3 of the LOPD provides that "consent to transfer of personal data will be invalid when the information provided to the data subject does not allow him to know the purpose for which the data the transfer of which is authorized will be used, or the nature of the business of the one to whom the transfer is to be made." The draft for these purposes indicates that when consent of the data subject is requested for transfer of his data, the data subject must be informed in such manner that he unequivocally knows the purpose for which the data with respect to which consent to transfer is requested are to be used, and the nature of the business conducted by the transferee. Otherwise, the consent is invalid. It is notable that the draft applies the expression "unequivocal" not to the consent (that there be no doubt, that there be no error), but rather to the purpose, which for us is expressed by the adjective "specific." If the consent to processing is not limited to a specific purpose, the consent is deemed not to have been given: "Otherwise, the controller will be deemed not to have obtained the consent of the data subject to the processing of his data." Under the draft, it would not be a problem of breach of the information principle, but rather one of lack of consent, which is debatable.

The draft regulations expressly provide that the processing controller is responsible for proof of the existence of consent of the data party, which may not be presumed. They affirm the principle that the burden of proof is on the controller. Nevertheless, the draft regulations include a procedure for the processing controller to request and obtain tacit consent of the data subject, provided that the LOPD does not require express consent. The draft regulations are particularly interesting in this regard. They go into very specific detail, facilitating compliance by the controller with the principle of consent, thus giving him legal certainty to know that he is acting correctly. Absolute proof of tacit consent would be impossible. For this

reason the draft regulations establish a set of deciding factors in this regard. One element of tacit consent is that the controller advise the data subject of the purpose of the processing and satisfy all requirements set forth in art. 5 of the LOPD, giving the data subject a term of 30 days to refuse the processing. It is very important to note that the draft regulations provide that in the case of controllers that send data subjects periodic invoices, the notice may be given together with the invoice for the services provided. It is very important that the file controller be able to determine whether the notice has been returned for any reason, in which case the controller may not process the data related to that data subject. In any event, the data subject must be given a simple means, involving no revenue for the processing controller, to refuse the processing of the data. In particular, such procedures are lawful if the refusal may be effectuated by a prestamped mailing to the processing controller or a telephone call to a free number or to such customer service facilities as the controller may have established. These two procedures have the advantage not only of resulting in no revenue to the processing controller, but also resulting in no expense for the data subject. In any event, as means for the data subject to refuse processing, the draft regulations only prohibit the sending of certified letters or similar messages, the use of telecommunication services that imply additional fees to the data subject or any other means that imply additional cost to the data subject. In any event, requiring the sending of certified letters, by contrast with additional fees for telecommunications services, does not result in revenue for the processing controller, but of course does result in inconvenience for the data subject.

The draft regulations also cover the request for consent when there is a contractual relationship, for purposes not directly related thereto. Thus, it is indicated that if the processing controller requests consent of the data subject during the process of contracting for purposes that are not directly related to the maintenance, development or control of the contractual relationship, he must allow the data subject to expressly refuse processing or transfer of data. This provision is related to the reference to free acceptance contained in the rules regarding processing of data of the parties to a contract or precontract for a business, employment or administrative relationship. Thus, the obligation is deemed to be satisfied when the data subject is allowed to mark a clearly visible box not already marked in the document that is delivered to him in the process of entering into the contract, or when an equivalent procedure is established allowing him to refuse processing.[50]

[50] In the section called "processing of invoicing and usage data regarding electronic communications services" the draft regulations cover the application for consent for processing or transfer of usage, invoicing and localization data by those subject to specific telecommunications regulations. The draft regulations are applicable to the extent not contrary to those regulations.

Very interesting are the provisions of the draft regulations covering the procedure for revocation of consent, an instrument intended to be different from exercise of the right of cancellation. If no special requirement is established for requesting consent, it makes no sense to establish one for revocation. It is stated that the data subject may revoke his consent using a simple means that does not imply any revenue for the processing controller. The same criteria are applied as for requesting consent. The controller will cease processing data within a maximum term of 10 days after receipt of the revocation of consent, without prejudice to his obligation to block the data as provided in article 16.3 of the LOPD. When the data subject requests that the processing controller confirm the cessation of processing of his data, the controller must expressly reply to the request. If the data have already been transferred, the processing controller, once the consent is revoked, must so notify the transferees within the term contemplated in section 2, so that they will cease processing the data if they still have it.

3

Regulatory Development of the LOPD from a Business Perspective

Belén Veleiro
Director of the Legal Department of the Superior Council of the Chambers of Commerce

Introduction

It is a fact that personal data protection over recent years has drawn increasing interest from Spanish companies. They are beginning to be aware of the need, pursuant to the current legislation on the matter, to implement measures ensuring the fundamental right of individuals to their personal data. In the business sphere these are reflected basically in the personal data of customers, employees and suppliers.

This is due to various factors, among which the following may be noted.

In the first place, personal data protection already has a lengthy tradition in our country. The former Organic Act 5/1992 of 29 October 1992 regulating the Automatic Processing of Personal Data (LORTAD) was based in article 18.4 of the Constitution, Council of Europe Convention 108, the Schengen Agreement of 14 June 1985 and the draft directive of the European Union regarding the matter. Ultimately Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 appeared, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The result of implementation of this directive was the approval of Organic Act 15/1999 of 13

December 1999 on Protection of Personal Data (LOPD) and Royal Decree 994/1999 of 11 June 1999 approving the Regulations on Security Measures for automated filing systems containing personal data. Constitutional Court judgment 292/2000 of 30 November 2000 recognized the existence of the fundamental right of data protection as an autonomous right consisting of the power of disposition of or control over the personal data of the data subject.

Complying with data protection regulations is an obligation of all companies that maintain and/or process files containing personal data unless otherwise stated it is an obligation of almost all companies. The challenge is complying with the objective of achieving a competitive market advantage, rather than an obstacle to normal operations of the organization. Society is beginning to be aware of the value of personal data and protection of it by companies results in higher quality which is perceived by the customer. Despite the great effort that is required in complying with these regulations, we must not forget that we are dealing with a fundamental right, recognized in the Constitution and protected by an Organic Law.

In the second place, from the entry of the first of the provisions regarding this matter, Organic Act 5/1992 of 29 October 1992 regulating the automatic processing of personal data, adapting Spanish legislation to the system established in the subsequent 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, until the current regulation established by Organic Personal Data Protection Act 15/1999 of 13 December 1999, the Spanish Data Protection Agency (AEPD) has not ceased in its efforts to make citizens and companies aware of the rights and obligations respectively applying to them.

In the third place, the figures are compelling: an average of 1000 violation files processed each year by the AEPD, resulting in sanctions for violation of rights of some 19,669,170.72 euros, the sanctions varying between 601.01 and 601,012.10 euros, which is beginning to increase the attention paid by Spanish companies to this matter.

Finally it is worth noting the decisive actions of entities like the Chambers of Commerce. In this regard, for the Chambers of Commerce the new technologies are an indispensable resource enhancing competitiveness and productivity of companies. From a business point of view, it is essential to implement Information and Communications Technologies (ICT) in the production process and business development on the appropriate conditions of legal certainty and free competition.

The actions undertaken by the Chambers of Commerce regarding the Information Society are within a global strategy based on two fundamental pillars: promotion of the New Technologies within Spanish companies, particularly small and medium-sized businesses; and the provision of value added services to companies regarding the Information and Communications Technologies. This is demonstrated by companies in which the Chambers of Commerce have interests, such as Camerdata (databases of business interest), Camerfirma (electronic signatures) and Camerpyme (online business services), and projects to implement the Information Society within companies, such as digital signatures, Nexopyme and the current concession to the public company Red.es to act as a supplier of alternative dispute resolution services for ".es" domain names, and the participation of the Superior Council of Chambers of Commerce as a member of the Advisory Committee on Telecommunications and the Information Society.

The Spanish Data Protection Agency could not be isolated from these activities. Since its creation, in the early 1990s, the Chambers of Commerce have maintained intense and fruitful cooperation with it. Appropriate management of the information that companies use and need has resulted in a sustained cooperation effort in various forms, among which it is appropriate to note: implementation by the Chambers of the established regulatory obligations, even knowing that most of its files are not subject to the regulations; entering into various cooperation agreements; the organization of many training and informational events for companies; mutual help in the development of activities; intensive training of Chamber technicians to facilitate providing appropriate information to companies; etc.

Some six years after approval of Organic Personal Data Protection Act 15/1999 of 13 December 1999, the Ministry of Justice and the Spanish Data Protection Agency (AEPD) are working on draft regulations in development of certain aspects of the Act. The initiative for the first regulatory development of the LOPD comes from the AEPD. In its 2003 Report it already referred to the need to undertake this project.

Throughout 2005 various work projects were undertaken with the participation of the sectors most affected by the draft regulations. Since the first contacts with the Ministry of Justice the AEPD has been pushing this regulatory development so that within coming months these development Regulations will be published and approved, thus replacing Royal Decrees 428/1993, 1332/1994 and 994/1999 and various complementary Instructions and rules.

The regulations proposed by the AEPD will be the result of experience acquired over the years, in light of the consolidation of information and communications

technologies and the difficulties of implementing the rules due to ignorance thereof.

Since exhaustive analysis of the many articles of the draft regulations would be too much, I will concentrate on the most significant or relevant aspects that, for practical purposes, may affect the daily life of the sectors involved, particularly companies.

The text, which develops points already established in the LOPD and also creates new concepts, is structured in three clearly differentiated parts. The first sets forth the most purely organizational and legal developments. The second part centres on technical aspects. The third part covers procedural aspects.

While it is not yet known with certainty what the transitory application of the rules will be, it is possible that the complete regulations will become effective upon their publication. It is also possible that the enforceability of the provisions therein temporarily will be different, in order to allow familiarity with the regulations and adaptation of businesses over a prudent period of time.

The regulations developing the LOPD

As noted earlier, the AEPD is promoting preparation of a text developing the LOPD. It will be based on consultation with and participation of the various sectors involved, and also a result of the experience acquired over recent years.

Without prejudice to possible changes in the proposed text that may be incorporated after study, drafting and consultation, as a starting point some of the proposed lines are set forth below.

In the first place, it is appropriate to note that the proposed text of the draft regulations fixes as their *scope of application* automated, unautomated and partially automated files; contact data; and a concept that the LOPD left unsettled: data processors located in Spain even if the data controller is not resident in Spanish territory.

Within the section for processing excluded from the scope of application of the regulations, there is a new item referring to the possibility that interested parties may apply to the AEPD to verify the lawfulness of data processing in cases of investigation of terrorism and other serious forms of organized crime. The AEPD may request cooperation of the file controller in undertaking the verification, limiting itself to replying to the interested party regarding undertaking the processing, but without any indication about the result.

As regards remission to specific provisions applicable to certain files it is notable that three new circumstances are incorporated. They refer to personnel qualification reports within the armed forces, data taken from the Civil Register and the Central Register of Convicts and Rebels, and the use of video cameras by state security forces.

Particularly notable among the principal innovations in the draft regulations is a specific *definitions* article. This is seen as a necessary complement in the Act, containing amendment or clarification of some terms already contained in the LOPD and introduction of other new ones.

Specifically worth special mention are the definitions of "Blockage" and "Erasure" of data. The draft contemplates the possibility of computer blockage of data to prevent processing, with a guarantee that they can be recovered by the government, judges and courts in order to attend to any responsibilities arising from the relationships of data subjects with them. As for erasure of the data, the draft does not allow physical elimination of data directly. Rather erasure follows blockage of the data and passage of the statute of limitations regarding responsibilities arising from the relationships of data subjects with the authorities. In addition, a distinction is made between the file controller and the processing controller, as separate figures.

As regards *consent and the information obligation* applicable to the file controller, the two have been consolidated as one of the principal obligations regarding data protection. Data protection clauses incorporated in contracts, forms or any other means of collecting data are a clear example of the importance of allowing the data subject to freely consent and express his agreement regarding any processing, purpose or destinee of the information.

Under the LOPD file controllers have the obligation to expressly, accurately and unequivocally inform interested parties from whom they request personal data regarding certain matters which, based on the draft regulations developing the LOPD, would be extended to an additional two:

— Inform regarding the type of business of the transferees or categories of transferees.
— Inform using a medium that allows evidencing satisfaction of this obligation.

Under the proposed text, only if the data subject is aware of and accepts all of these circumstances may we speak of the existence of true consent. The file controller is also required to prove the existence of consent. It never can be presumed.

Regarding the manner of obtaining consent, tacit consent is considered to be valid,[1] unless the law requires the processing controller to obtain express consent. Nevertheless, a series of requirements are established for obtaining consent:

— The data subject must be given a term of 30 days to state his opposition to processing, if he so wishes.[2]
— The data subject must be given a simple means of stating his opposition, at no additional cost nor may it imply additional revenue for the processing controller.[3]
— The processing controller must determine whether the notice has been returned for any reason. In that case, the data may not be processed.
— The processing controller may not process or transfer the data until at least 45 days have passed after the date the notice was sent.

Regarding revocation of consent, it also is subject to a series of requirements:

— The processing controller must provide a simple and cost free means of revocation, that does not imply any revenue to the processing controller
— The processing controller will cease processing within a maximum term of 10 days[4] after receipt of the revocation, and
— He must expressly reply to the application presented by the data subject.
— If the data have already been transferred, the controller must notify the transferees of the revocation, within the same term.

Nevertheless, consent is not necessary in certain cases. Although they already have been exhaustively listed in the LOPD, the draft regulations state them succinctly. In this regard, of special relevance is the exception to the consent obligation when it refers to the parties to a contract or precontract regarding a business,

---

[1] The AEPD, in a Report of the year 2000, stated that: "consent may be tacit in the processing of data that are not specially protected."

[2] In the case of controllers that send data subjects periodic invoices, the notice may be given together with the invoice for the services provided.

[3] The draft regulations accept a procedure whereby the opposition may be stated by a pre-stamped mailing to the processing controller, or a call to a free telephone number or the customer service department. Not acceptable as means for the data subject to state opposition to processing are the sending of certified letters and the like, the use of telecommunications services that imply additional fees, or other means that imply additional cost.

[4] For these purposes, the term must be understood to refer to working days.

employment or administrative relationship, with respect to the data that are necessary for proper maintenance, development or compliance.

All of the foregoing regarding consent to processing and transfer of data applies provided that they are not specially protected data. Generally speaking, specially protected data may be processed and transferred only with prior written consent of the data subject, a legally imposed authorization in the general interest, or a directly applicable rule of community law.

Regarding regulation of the information obligation, a distinction is drawn between data collected from the data subject himself (in which case he must be informed in advance) and those not collected from him. In any event, this obligation must be fulfilled using a means that allows evidencing that it has been satisfied, to be preserved for so long as the data processing continues.

Another of the innovations incorporated in the new regulations affects the *data processor* when the file controller's processing of the data is undertaken by a third party company. In this case it is always required that the relationship be properly set forth in a written contract stating the scope of the assignment, what security measures will be applied to the data, a prohibition of using them other than for the contracted purposes and a prohibition of transferring them to third parties.

This relationship sometimes includes subcontracting. Thus, it is provided that the data processor may subcontract with a third party for the processing, either with a sufficient power of attorney from the file controller, and on its behalf, or without need of such a power of attorney, under the circumstances described below:

— Specification in the contract of the services and the subcontracted company.
— Processing of the data by the subcontractor in accordance with the instructions of the file controller.
— Formalization of the contract in accordance with article 12 of the LOPD, between the data processor and the subcontractor.

Lastly, regarding subcontracting, the draft regulations establish the obligation to redirect, to the file controller, any request from the data subject regarding the rights of access, rectification, erasure or opposition, if received by the data processor.

Once the contractual services are completed, the LOPD already establishes the obligation of the data processor to destroy or return the data to the file

controller. Nevertheless, the draft regulations include two clarifications. They allow dispensing with destruction of the data if, by reason of a legal authorization, their preservation is required, with a guarantee of the file controller in that regard. They also allow blockage by the data processor to support possible liability in its relationship with the file controller.

Another of the matters developed by the draft regulations is the right of each individual to dispose of his own data, that is, the specific regulation of the *rights of access, rectification, erasure and opposition.* Among the innovations, the following should be noted:

— The controller is required to provide a simple means of exercise of these rights.
— The exercise of these rights may not result in additional revenue for the controller.
— The controller must respond to requests made by data subjects provided that they have used means that allow proof of the sending and receipt of the request. The burden of proof is reversed, requiring the data subject and not the controller to evidence sending by certified letter or similar means.
— An express statement is made regarding the term established for the processing controller to effectuate the rights. If stated in days, they must be understood to be working days.
— The obligation of the file controller to inform the data subject of his right to apply for protection of the Spanish Data Protection Agency when the right is denied.
— As regards the right of opposition, data subjects are entitled not to be subject to a legally binding decision with respect thereto, or a decision that significantly affects them, based on automatic processing of data to evaluate certain matters, such as their work performance, credit, conduct, etc.
— In addition each right is specifically regulated as regards exercise with respect to specific files (solvency and credit, advertising and marketing, medical histories).

The draft regulations continue by regulating security measures, analysis of which will be given a specific section by reason of their direct effect on companies. The draft then refers to obligations prior to processing data (notice and registration), and a certain files in great detail, beginning with publicly-owned files, files with information regarding solvency and credit, those related to monetary

obligations, advertising and marketing files and files from sources accessible to the public.

There also is detailed regulation of model codes. These, of a voluntary nature, by sector or individual, are deposited and published by the AEPD. They must include certain minimum content complying with the regulations and certain additional commitments. Specifically regulated are supervision thereof and the obligations of the entities promoting them.

There also is detailed regulation of international data transfers. A distinction is drawn between those that are made to States that grant an adequate level of protection, and those destined for territories that do not grant that level of protection. Most of the latter require authorization of the Director of the AEPD and compliance with more specific requirements.

There also is very detailed regulation of actions of the AEPD, from preparation of Instructions to protection of rights of access, rectification, erasure and opposition, those related to the exercise of its sanctioning authority, those related to registration, amendment or erasure of files, ex-officio cancellation of registered files, authorization and temporary suspension of international data transfers, preparation of model codes, extension of the information right to data subjects, authorization of preservation of data for historical, statistical or scientific purposes and publicity of its resolutions.

Principal innovations regarding security measures

The draft regulations maintain the existing three levels of security (basic, medium and high). The draft is structured into three sections for the description of each of the levels of security: general measures for all files, measures applicable only to automated files and measures applicable to non-automated files.

In general as relates to security levels, it is worth noting that the "lower medium" level for employment profile files disappears. They are directly transferred to the medium level together with files regarding those under 14 years of age, files for which the Social Security Administration is responsible and files containing data related to victims of sex crimes. Also notable is the introduction by the new draft of an express provision for periodic controls to be applied to the Security Document.

Regarding the basic level of security, a series of general measures is established, regardless of whether the file is automated or non-automated. The principal innovation in this regard in the draft is that it applies not only to computer

media, but also documents. The result may be that even paper documents leaving the company containing personal data (payrolls, contracts, etc.), or e-mail including such data, must be registered, the transfer being authorized when it occurs or by establishing a provision in this regard in the security document. The regulations also require incorporation of measures for storage and archiving of paper documentation.

Amendments are also introduced regarding identification and authentication. Biometric data may be used to identify file users. It is provided that replacement of passwords will be undertaken within a term not greater than one year. The Security Document may establish a shorter time period. For automated files, the regulations require the file controller on a semi-annual basis to verify the conduct of operating tests and application of procedures for backup and recovery copies.

Regarding medium level security, the mandatory audit to be undertaken at least every two years of medium and high level files is maintained. It must be performed provided that there have been significant changes in the information system, to verify the adjustment, adaptation and effectiveness thereof. The person appointed as auditor must have an appropriate employment profile and experience. He may be a member of the organization. In this case he must function independently of the audit area. He also may be a third party specialized in review of information systems. If neither of these situations is possible, the one responsible for conducting the audit will be an independent agent. His appointment must be notified to the AEPD, as must the date of the audit.

Regarding medium level measures for automated files, we must mention the new provision that requires encryption of data when they are stored on portable devices.

Regarding high level measures, the data must be encrypted to avoid access or manipulation when they are distributed. Data on portable devices also must be encrypted when they are away from the facilities of the file controller. For non-automated files, sensitive data of that level on paper must be stored in cabinets or filing systems locked with a key or similar device. Until all of this information is archived, a person must be appointed to guard the information during all of its processing. In addition, if there is a transfer of file information on paper, measures must be adopted to avoid its manipulation, as must controls that allow detection of any unauthorized access.

Latest actions of the AEPD

In addition to promoting regulatory development of the LOPD, the AEPD has concentrated on other matters of interest. Particularly important among the latest innovations is Instruction 1/2004 of 22 December 2004 on publication of its Resolutions. One of the fundamental objectives of the AEPD is achieving greater transparency in its actions, within the framework of the process of implementation of the Information Society, to better guarantee and protect the fundamental right of personal data protection.

Organic Data Protection Act 15/1999 of 13 December 1999, after the amendment introduced by article 82.1 of Act 62/2003 of 30 December 2003 on Tax, Administrative and Social Order Measures, in its article 37.2 provides that AEPD resolutions, with the exception of those corresponding to registration of a file or processing in the General Data Protection Register and those ordering registration therein of the model codes regulated in article 32 of that Act, will be made public after notice has been given to the data subjects, preferably using informatics or telematic means.

This strengthens publicity of criteria for application of the data protection regulations and promotes application of the principles of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Continuing with this objective of publicity and transparency, the AEPD has made available to the general public[5] a model security document addressed to file controllers and personal data processors, in order to encourage general compliance with the principle of security of personal data.

In addition, spam, junk mail and unsolicited communications sent by electronic means are intended to offer or market products, goods or services, accomplished by electronic means, generally via e-mail. The AEPD also has jurisdiction regarding this matter.

Sending this kind of message without prior consent of the addressee is prohibited by Spanish legislation, both Information Society Services Act 34/2002 and Organic Personal Data Protection Act 15/1999 of 13 December 1999.

Widespread use of this practice has its origin in the low cost of the messages, whether via Internet using e-mail or by other means such as mobile telephony

[5] www.agpd.es

(SMS, MMS), the anonymity that is possible, the speed with which the messages arrive and the large number of addressees and possibilities as regards content.

The Information Society Services Act (Ley de Servicios de la Sociedad de la Información—LSSI) expressly prohibits sending commercial advertising or promotional communications via e-mail or other equivalent electronic means if not requested or expressly authorized in advance by the addressees thereof, unless there is a pre-existing contractual relationship and the communications relate to similar products or services. Such conduct is sanctioned as a minor or serious violation. But it also may imply violation of the right of privacy and the personal data protection legislation. This is because in certain cases e-mail addresses have been held to be personal data.

As has been noted, the laws that regulate the unsolicited sending of electronic commercial communications, such as Information Society Services Act 34/2002 and General Telecommunications Act 32/2003, give jurisdiction over this matter to the AEPD. It is responsible for protection of the rights and guarantees of subscribers and users in this area, with authority to impose penalties in the event of violations occurring by reason of sending unsolicited commercial communications via e-mail and other equivalent means (SMS, MMS, phishing, pop ups, hoaxes, scams, etc.).

Spam is about 70% of world e-mail traffic. It is one of the elements that destroy user and consumer confidence in the Information Society. If one learns of the country from which spam is issuing, the corresponding authorities must be advised, in order to prosecute this conduct.

By the very nature of the Internet and the electronic media used for spam, international participation is required. For this purpose the EPD is signing various cooperation agreements (United States, Latin America and the EU). In the case of the United States the unsolicited messages may be transferred to the US Commerce Department. The Spanish Data Protection Agency recently signed a cooperation agreement with it.

In addition, 13 European Union data protection authorities have signed various agreements whereby, when they receive complaints from other signatory countries regarding the existence of spam issuing from their territories, they are required to exert maximum efforts to detect and combat the source complained of. These countries are Spain, France, Italy, Belgium, Cyprus, the Czech Republic, Denmark, Austria, Ireland, Lithuania, Malta and Holland.

In addition, the AEPD also has had a significant role in the implementation of the DNIe. This is an initiative of the government to promote development of the

Information Society in Spain. The basic objectives are electronic evidence of the identity of citizens, giving the national identity document (DNI) an electronic signature function, and improving service to the citizenry by providing issuance and delivery of the document at the time of application.

Thus the government, showing its sensitivity regarding the implications of the DNIe on personal data processing, has sought the cooperation of the AEPD, which thus has participated in the Coordinating Committee created for that purpose. In this regard, regarding the quality of data and proportionality, the data to be contained in the DNIe will be the same as in the current DNI. Thus, in the AEPD's view they are consistent with the principle of proportionality, as they are adequate, pertinent and not excessive for the purpose pursued.

One of the topics that has been most debated, having been considered by the Information Society Commission and the Senate, is the possibility that the DNI may include additional data, such as the drivers license or health data. In this regard, in the AEPD's view a document incorporating such additional data would be a document distinct from the DNI, and would require new legal authorization in order to be implemented and developed. It is a matter of avoiding the existence of a unique identification number for each citizen, with which it would be possible to access many of their data. It might facilitate matters, but also could result in many risks to privacy.

In the European Union there is no uniform generalized system. Finland was the first country to begin to use a similar document. In 2000 it began issuing the document, later incorporating a social security identification function. Belgium initiated the project, (not including biometrics) at the same time, contemplating its generalization in 2008. Nevertheless, in countries like the United States, England, Ireland, Sweden and Norway, in which there is not even an identity document, when the possibility of using an identity document has been proposed there has been strong popular opposition, considering it to interfere with the privacy of citizens.

Conclusions. Impact on business

Given the situation and current status described above, it is undeniable that, as we stated at the outset, protection of personal data in our country enjoys an undebatable tradition, to which one must add the actions undertaken by the AEPD. But it also is to be noted that Spanish regulations imply significant obligations and

high penalties for noncompliant companies, which are not reflected in the regulations of other countries in our environment[6].

Although it is clear that regulatory development of the LOPD is necessary to introduce a greater degree of legal certainty, it cannot be done on the backs of the sectors most involved, that being companies. Particularly when Spanish legislation does not make compliance easy, for small and medium-sized businesses or for those having greater resources.

It cannot be questioned that the draft regulations developing the LOPD that are being prepared will impose new and significant obligations on companies and will change many of those currently applicable to them. This implies an extensive technical, organizational and economic effort.

We will highlight some of the proposals of the draft that will most affect business activities and the daily life of companies.

In the first place, it is worth noting that non-automated files will be covered. Temporary files that, up to this point, have been understood to be files created for a limited period of time, for a specific purpose, and/or drawn from a computer file previously created by the organization itself, will also be covered. The draft regulations establish a broader concept. They cover working files created not only for occasional processing, but also created as an intermediate step during processing. Companies must comply with the pertinent security measures with respect thereto.

They also include contact data as personal data. Since they apply to non-automated files, they apply even to the card holders typically used to keep track of personal contacts, which must be audited in accordance with the described requirements.

As regards consent, the obligation to inform data subjects using a medium that allows evidencing compliance and preserving that evidence poses problems for certain companies with small facilities. In addition, the requirement of evidencing satisfaction of the information obligation also applies to the request to obtain consent, which must refer to specific processing, stating the purpose for which the consent is sought, and must be proven by the file controller.

It is the file controller that must maintain proof showing the existence of consent: a) that the data subject has been informed of the matters listed in the law and regulations; and b) that the data subject has consented to processing of his data.

---

[6] The Superior Council of Chambers prepared a comparative document of data protection legislation in European countries. The result shows that Spain is one of the countries that imposes the most obligations on companies, especially as regards security measures, and imposes some of the highest penalties.

For example, the obligation to allow data subjects to refuse processing for purposes not directly related to performance or maintenance of the contract, by marking boxes or an equivalent procedure, implies separate treatment for each contract of the data protection clause or instrument that is used, so that the data subject may in fact determine the purposes for which he does not wish to give his consent.

The described security measures and their adoption by companies would present difficulties in implementation of an organization's processes, for example consultation by personnel of archives, file cabinets or libraries, particularly if they must be kept locked. To this add the need to amend many of the contracts the companies have already entered into, for example with security, maintenance and cleaning companies, etc. These would include clauses regarding prohibition of accessing personal data and the secrecy obligation regarding the data they learn in the process of rendering services.

As regards the security document, the file controllers must, among other obligations, show each event of processing undertaken by the data processor on its premises. On the other hand, if the services are rendered outside the premises of the file controller, in addition to the controller himself, it will be the processor that must show the processing in his own security document.

Generally, the full content of the organization's security document must be reviewed. An example of a special case is the need to foresee the prior authorizations required for taking portable devices (PCs, notebooks, etc.) from the premises, which represents great difficulty for companies.

4

Corporate Governance: Voluntary Compliance with Personal Data Protection Legislation

Javier Puyol
Director of the Corporate Litigation Department of the BBVA Group

Over recent years, the Sarbanes-Oxley Act, also known as SarOx or SOA, has been the law regulating financial and accounting audit functions and harshly penalizing corporate and white collar crime.

The Act has conditioned and continues to condition the legal system within which companies operate. Therefore data protection cannot be an isolated matter. The Act was a result of multiple frauds, management corruption, conflicts of interest, negligence and malpractice of some professionals and executives. Knowing the codes of ethics affecting them that should have governed their professional conduct, they succumbed to the attraction of earning easy money through companies and corporations, defrauding shareholders, employees and interest groups, among them customers and suppliers.

The application and interpretation of this law has resulted in multiple controversies. One of them relates to the extraterritoriality and international scope thereof. It has created a certain panic in the world financial system, especially banks that operate in the United States and multinational companies traded on the New York Stock Exchange.

Taken together this has significantly affected both the development of the Information Society and improvements in communications. New applications and

tools have been created allowing evolution and taking maximum advantage of traditional business processes. This has facilitated, for example, a clear increase in productivity and a substantial improvement in relationships with and knowledge of customers, all thanks to information.

As a result, all information, of whatever nature, has become a legal asset of extraordinary value. It must be guarded and protected. Thus, from a corporate point of view it cannot be separated from ethical values.

Not only does it promote significant new economic interests. It is also an indispensable element of development of multiple initiatives, both public and private.

There are many who now characterize information as the real power in advanced societies.

States, associations, companies, and even general citizens are more or less powerful to the extent they have access to large volumes of information.

Knowledge in general, and scientific knowledge in particular, now demand processing and the evaluation of multiple and diverse, and above all very complex, sources of information having very different characteristics and influence.

Therefore, a policy that attempts to establish or in fact establishes indiscriminate limits or conditions on access to information is difficult.

For its development, as it is viewed today, society demands ever more data and information. Consequently, knowledge has become an absolute value in and of itself. It has not been possible to isolate data protection from it nor, therefore, the business world.

In this regard it is worth noting that both statistical studies and market research have become indispensable to the development of many industries and commercial and industrial activities. They cannot be developed and implemented without having broad advance information based on multiple data, many of which affect or may affect the privacy of individuals, because they are personal to them.

In this context we must emphasize the economic processes of production and distribution of goods and services, which are inconceivable in a technologically advanced and developed society without prior knowledge of the datum, the statistic, the percentage, and other similar elements with analogous characteristics and natures. Today it probably can be stated without much room for error that the greatest asset held by any company is its own customer base. That is, the specific personal data it uses regarding its customers, shareholders and suppliers, which both drive development of its business and obviously affect any future expectations with regard thereto.

Many of these data, reports and items of information apply or have effects in the area of the personalities of citizens, their personal and family privacy, the ultimate refuge for "privacy," what "belongs" to me, what is "mine." And all of this as against the same interests of others. We must recognize that all of this may be decisively affected by a society and by market rules that, as currently structured, demand and consume a great amount of information and at times pay no heed to the existence of individual rights, which in any event should prevail and be respected.

It is a fact that information, in its broadest sense, whatever it is about, including information revealing private aspects of one's personality, basically has become a commodity. In this sense it may be said that there is an authentic social demand for information. By way of example we may mention politicians, investors and businessmen who need ever-increasing information in their work. This even can be said of the citizen himself, in the most anonymous sense, since he spends a great part of his leisure time in consuming information.

Ultimately any human or social activity, as has already been stated, requires sufficient and necessary knowledge to allow proper development.

Thus, one can understand that a democratic society in which the State, characterized, inter alia, as representing "social" interests, may assume a belligerent position in defence of the rights of individuals, and cannot remain indifferent to or apart from the dialectical tension between two values that traditionally have been considered at odds:

a) On the one hand, the so-called consumption of information, and
b) On the other, the necessary and indispensable defence of the personality of the individual.

Both terms of the pair are quite uncompromising:

a) Freedom of information, of which IT freedom is the typical exponent, which is offered to us as a necessary component of a free, pluralistic and egalitarian society.
b) Defence of the citizen and his personal and family privacy as a politically legitimizing characteristic of any democratic society.

In the light of all the foregoing, we may reach the conclusion that IT freedom is a legal right increasingly demanded as a commodity in advanced societies, and

that it is inconceivable without being countered by safeguarding or defending personal data affecting personal and family privacy.

That right is established based on the idea of privacy, and consists of including a dynamic supervisory function for information related to the individual.

This objective is achieved using the technique of data protection consisting of nothing more than a set of subjective rights and obligations and objective procedures and rules.

This gives the individual, the beneficiary, a status that allows defining "the degree to which he wishes to have his identity and circumstances known and circulated, combating inaccuracies or falsities that alter them and defending himself against any abusive use" attempted to be made of them.

In this way, the guarantee of privacy may adopt a positive content in the form of the right to control data regarding the person himself.

The so-called informatics freedom thus also is a right to control use of personal data loaded in a computer program, the so-called "habeas data."

In this regard, going a step further, it is worth asking whether compliance with regulations regarding data protection is something merely imposed by the current legal system, or whether on the other hand compliance with these legal and ethical rules may even be profitable for a company.

And the answer to this question in our opinion must always be affirmative.

A market that is regulated as regards data protection implies that all participants in that market start from an equal position, from a similar regulatory framework they necessarily must respect.

Therefore both the current Organic Data Protection Act and the rules currently complementing it, as well as the future regulations in the final phase of preparation must always be favourably viewed by the market. This is because they establish equal operating rules for all competitors, imposing on all of them the effective bases for legal certainty so that all who wish or need to participate therein may effectively compete.

The European model, implemented by means of a strict system and many directives, by comparison with the systems that propose no regulation, or even self-regulation, common in the Anglo-Saxon system, have resulted in appropriate development of the market. It is marked by the balance and legal certainty that should govern normal development of business activity, and at the same time respect the rights of customers, shareholders, suppliers and the general citizenry.

In our opinion, this never will be harmful to companies that, respecting these rules of the game, promote greater transparency of information, total respect for

the rights of citizens, and create a suitable atmosphere of legal certainty, making the necessary effort not only to be the best and most competitive, but with that not implying any decrease in compliance with ethical business values. For the market, without any doubt, it will be an economic and social model that ultimately will be rewarded.

Respecting the legitimate rights of customers, shareholders, suppliers and all those whose personal data ultimately are involved in the productive system, making the practices that relate to them available transparently with the conditions of their organization, their operating system, the procedures that are to be applied, the security rules for the environment, the programs or equipment that will be used, the obligations assumed by those involved in processing and use of personal information, the guarantees (as indicated by the current Organic Data Protection Act) that are established within their scope of operation for exercise of the rights of individuals, all of these are fundamental aspects of these ethical and legal provisions.

All of this means that full respect for the principles and regulations of informatics freedom and the regulations implementing that fundamental right is not only ethically desirable, but acting in this manner is certainly economically more profitable from multiple points of view.

Finally, we believe that application in any company of ethics rules or codes of internal conduct regarding data protection not only strengthens its legal position in this regard, constituting a clear example of good corporate governance, but also from a strictly economic point of view ends up as a clear and definite profitability factor.

Compliance with these rules means placing the customer at the centre of the business, providing it with quality services, fostering the customer's personal and professional growth and business development. Ultimately, it satisfies the customer's needs, responding more effectively to the customer's expectations, concentrating the business on the relationships established over the long term based on confidence, respect and the reciprocal value arising for the customer and the company from this framework of legal certainty, ethics and transparency.

In this order of things, compliance with these rules must always be attributable to the overall business, not just a part of it. Every day there must be greater conviction that respect for these principles must be a part of all projects, units and persons included in a company.

In this consciousness-raising work it is appropriate to recognize the significant transformation occurring within the corporate structure and the citizens of our country. This no doubt is the result of the successful work raising awareness of

and applying the Act. This has been accomplished over these years by the government through the Spanish Data Protection Agency. Although it is evident that much remains to be done, what is being achieved is that compliance with the data protection regulations themselves has evolved from being just a mandatory matter of a legal nature to something that now forms a part of the culture of both companies and the citizens themselves. Both are increasingly conscious of their obligations in their activities and the rights corresponding to each of them, which necessarily must be respected by all.

From a corporate point of view this should lead to the adoption of awareness and management models for the organization that promote communication, and training in this regard for all those involved in an economic group.

Perhaps a basic element of communication is instilling respect for the principles and rules governing data protection as something not ethereal or abstract within the company, or imposed by the system, but rather a task that begins with and is of interest to each person, for their own benefit of that of the customer.

It is something that should arise from individual consciousness as a participant in the productive system, but also as a citizen.

For this purpose it is essential that the communication of these values be inextricably linked to a significant training effort, by means of courses, presentations, and anything else that strengthens this awareness model, resulting in this culture.

Nevertheless, sometimes it is not sufficient just to comply with legal provisions, particularly in cases like ours, where individual freedom and the rights of citizens are in play.

Here it is necessary to be rigorous and demanding in application of the practices that lead to good corporate governance of any company as regards data protection.

The guidelines to be followed must start with mandatory compliance with the requirements of applicable legislation, but not viewing compliance therewith as the end of the story.

Rather they should lead us to consider whether the principles of mandatory application are to be seen as the minimum standard established by applicable legislation, or if on the contrary it is a given that in each company additional guidelines for application of those principles or legal requirements may be established that improve and complement them.

This cannot be considered to be a burden, but rather respect for and strengthening of the individual freedom that must be paramount in all data processing.

This concern is applicable both to the specific principles that may underlie data processing in the sector or within the company, and to the development of procedures for application thereof, establishing new regulations for certain matters, or definitions that from a technical point of view improve the position of data subjects.

Application of these ethical principles appears in many ways, and relates to many legal provisions, among which by way of example we may cite, among others, the following:

— those affecting the classification of data to be processed;
— those affecting the sources, by lawful and fair collection of data;
— those affecting the data to be processed, always paying particular attention to their truthfulness;
— those affecting assignment of the data, and international transfers thereof;
— those affecting the existence of more restrictive disclosure clauses regarding collection of data;
— those affecting limited retention of data, with effective deletion when they actually cease to be necessary or pertinent;
— those affecting constant respect for the principle of consent, asking whether it must always or predominantly be express and verifiable;
— those affecting ready access by data subjects to legal and regulatory rights, including improvement of the conditions under which there are procedural grounds for exercise those rights.

The standards for good governance also may be fairly reflected in security measures of both a physical and informatics nature, always characterized by the commitment to first comply with the minimum measures contemplated by law, but also such degree of additional compliance as may improve the situation regarding processing of data of customers, shareholders and suppliers.

And all of the foregoing without prejudice to the establishment of binding corporate rules or even the creation of procedures for self-regulation and internal and external control and compliance with the applicable legal rules, which in turn may be of multiple and diverse content.

The legal system currently existing in the European Union, where not only does the existing legislation demand appropriate respect for data protection, but also it is necessary to recognize and praise the role being played in defence thereof by the respective national regulators, present here today.

All of this, together with the strengthening of informatics freedom based on this positive self-regulation, far from resulting in diminishment of the dynamic

nature of the market and the development of business, without doubt will result in improvement of the competitive nature thereof, and of the guarantee of individual rights of citizens. Protected by greater legal certainty they will increase their ties with the economic projects that better guarantee these ethical principles.

Part II

THE DATA PROTECTION DIRECTIVE AND GLOBALIZATION: THE SIGNIFICANCE OF THE DIRECTIVE

5

The Work of the Article 29 Working Party

Peter Schaar
Federal Commissioner for Data Protection and Freedom of Information
Chairman of the Article 29 Working Party of the European Union Data Protection Directive

I take pride in participating in this congress and it is an honour and a pleasure for me to speak to you, especially as Chairman of the working group of the European data protection authorities, the so-called 'Article 29 Working Party'. I want to give you some information about its history, role and work. I am particularly happy for the opportunity to speak on this conference, because I work closely together with my colleague José Luis Piñar Mañas, Director of the Spanish Data Protection Agency, who is doing a wonderful job as Vice Chairman of our WP.

Introduction and role

The Working Party (WP) was established in 1996 by Article 29 of Directive 95/46/EC on protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive). Members are the representatives of the supervisory authorities of every member state, the European Data Protection Supervisor and the European Commission. The Working Party is the independent EU Advisory Body on Data Protection and

Privacy. Since its establishment it has played a key role promoting harmonisation of data protection in order to achieve a high level of data protection in the EU, fostering compliance with the data protection standards set up by the Data Protection Directive and providing guidance and advice to the different actors in the data protection arena.

Its tasks laid down in Article 30 of Directive 95/46/EC are mainly:

— To examine any question covering the application of the national jurisdiction and of all measures under the directive in order to contribute to the uniform level of data protection and a harmonized enforcement of legal provisions all over Europe.
— To give an opinion on the level of protection in the Community and in third countries.
— To advise the Commission on any proposed amendment of the directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms.
— To inform the Commission if it finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member.
— To give an opinion on codes at Community level, so far as data protection is concerned.

The WP has no supervisory functions towards the national data protection authorities. But it brings the connection between the national institutions and the different experiences from all member countries. The aim is to harmonize the different data protection laws and practices and in this way to enforce privacy in all Member States. This is one of the main tasks for our work. Especially, after the Commission has published the First Report on the implementation of the Data Protection Directive in May 2003 [Com(2003) 265 final] the group has given priority to this work. In the report, the Commission has pointed out that there is a lack of adequate implementation of the data protection directive. The key-question is: How could we contribute to a better compliance with the directive in all Member States?

Up to now the group has adopted 118 opinions. They give guidance to supervisory authorities, help to harmonize the different laws and are also meant as

political statements to current data protection issues. These opinions cover a wide scope and refer to legal questions as well as to the challenges resulting of the fast development of information and communication technologies.

Several subgroups have been established to deal with special issues. They also prepare the plenary sessions by formulating draft opinions.

Additionally, the group published an annual report about its work. The Eighths Annual Report has been presented to the European Parliament on 21 February this year.

Cooperation with European institutions and bodies

One of the most important duties of the Article 29 Working Party is to give advice to the different European Institutions.

The European Commission is the institution with whom the WP works more closely as it has advisory powers to the Commission and its opinions must be sought before some Commission decisions are taken. Moreover, the Commission is a member of the group and also plays a fundamental role providing the Secretariat.

Furthermore over time, the relationship between the Working Party and the European Parliament has become closer and closer, with the latter endorsing most of the opinions of the Working Party in its Resolutions on data protection matters. The group believes this dialog and co-operation must be improved further as the European Parliament, representing the views and concerns of the European citizens, has always been very sensitive to the safeguarding and promotion of the fundamental right of data protection.

There is no special independent group for data protection in the Council. For this reason it seems to be very important to enhance the contact with the Council too.

Practical co-operation

Co-operation among data protection authorities is highly desirable, both in their daily operations and as part of the planning of joint actions, and must be a prominent component of any strategic plan or policy. Several instruments are now in place to foster practical and efficient co-operation among European data protection authorities and are current examples of this commitment:

The Case Handling Workshop was established by the European Spring conference and not only Member States of the European Union are taking part, but also other European countries. They are meeting twice a year and working on harmonization between the different data protection laws. They discuss special items of mutual interest. It is very important that also non EU Member States are taking part. The last meeting has just taken place in Madrid this week.

Additionally, the subgroup Enforcement is working in this field. Like the other subgroups it is working on special mandates of the WP. A questionnaire on data protection in health or in the medical insurance sector was prepared. It is the first time that the national Data Protection Authorities of the Member States undertake a coordinated EU-wide investigation with the help of this questionnaire. The investigation has started on 13 March. The responses received will be evaluated both at national and at EU level. Based on the results, the WP could subsequently decide to issue practical guidance for the sector at large and identify areas for future action.

Last year another subgroup was especially established dealing with the problems of PNR. This group is an example for a successful cross border cooperation. In September 2005 the first annual joint review took place in Washington. Members of the EU Commission and representatives of the national data protection authorities have participate in the review. It took a long time before it was possible to realize this project, but it was a success and led to a positive result.

Transfer of personal data to third countries

More and more the transfer of personal data to third countries has become one of the major topics in the field of data protection. The WP has given advice to the Commission during the procedure of recognition of adequate protection (Switzerland, Canada, Argentina). There is no general decision for the USA, but there is the possibility of Safe Harbour and sectoral decisions. During the last year the group has intensified the work for Safe Harbour. Last December the US Department of Commerce held a seminar on the Safe Harbour agreement in which also the Federal Trade Commission, representatives of the European Commission and the European Commissioners for Data Protection participated. I want to emphasize that the Spanish DPA contributed impressively to the great success of this workshop. Member States may also authorize transfer of data where the data controller offers adequate safeguards like Standard Contractual Clauses or Binding Corporate Rules.

Meeting the challenges of international terrorism

The last years of our work have been characterized by the lasting conflict between the attempts of European and foreign governments to implement new instruments in their fight against terrorism, on one side, and the need to defend data protection principles as an essential element of freedom and democracy, on the other side.

The transfer of passenger data (PNR) was only one of the issues that the group had to deal with. Last year there was also a long and fundamental discussion about the need for a European-wide preventive retention of traffic data.

Another item is the introduction of biometric features into personal documents as a reaction to worldwide security threats. The Working Party clearly defines data protection needs in all these cases and will go on doing so. During the next few years the fundamental discussions will continue.

In closing my contribution I want to emphasize our common aim to anchor data protection as a human right world wide. In this way we will be able to cope with all challenges, wherever they come from.

6

Data Protection in the European Institutions

Peter J. Hustinx
European Data Protection Supervisor

Let me start by congratulating you on the organisation of this First European Congress on Data Protection. As European Data Protection Supervisor, I can only be delighted about this event and hope that more will follow, reflecting an equally wide range of stakeholders in data protection as a basic requirement of a modern information based society.

European institutions, such as the European Commission, the European Parliament and the Council, are playing an important role in setting data protection standards for the, now, 25 EU Member States. Since a few years, such standards also apply at EU level, with independent supervision by a European Data Protection Supervisor (EDPS). After having been in that capacity for a bit more than two years, with my Spanish colleague Joaquín Bayo Delgado as Assistant Supervisor, I am happy to give a brief overview.

Background on the EU

First, a few general points of introduction. As an international organisation, the EU is not subject to national data protection requirements. Therefore, it

had to develop its own regime. The EU consists of three 'pillars', each a product of historical evolution with its own typical features. The 'first pillar' is the Economic Community with the longest history and most widely developed powers and activities. The 'second pillar' covers the international relations and common security policy. The 'third pillar' deals with police and judicial cooperation in criminal matters. These pillars are still largely intergovernmental in nature.

The European Union as a whole has to respect safeguards for fundamental rights, such as the European Convention on Human Rights, according to Article 6 of the EU Treaty—but the EU is not yet a party to this convention—or to Convention 108 of the Council of Europe on Data Protection. The protection of personal data has been recognized as a separate fundamental right in Article 8 of the EU Charter, adopted in Nice in December 2000, and the Constitutional Treaty has built on this basis with several provisions, but as you know, it has not yet been ratified.

Article 286 of the EC Treaty, inserted by the Treaty of Amsterdam in 1997, provides that Community instruments on data protection also apply to Community institutions and bodies, including the establishment of an independent supervisory authority. This inter alia refers to the general framework Directive 95/46/EC. Further rules have been laid down by the Parliament and the Council in Regulation (EC) 45/2001, which may be considered as implementation of the directive at EU level. This Regulation applies to processing of personal data by Community institutions and bodies, when they act—wholly or partially—within the framework of Community law. This is a reference to 'first pillar' activities.

The Regulation is the basis for my activities as European Data Protection Supervisor. It provides for three main roles:

— a *supervisory* role, to monitor and ensure that Community institutions and bodies comply with applicable legal safeguards whenever they process personal data;
— a *consultative* role, to advise Community institutions and bodies on all relevant matters, and especially on proposals for legislation that have an impact on the protection of personal data;
— a *cooperative* role, to work with national supervisory authorities and supervisory bodies in the 'third pillar' of the EU, with a view to improving consistency in the protection of personal data.

During the first two years, important progress has been made in these three areas. More and more EU policies depend on the lawful processing of personal data. Many public or private activities in a modern society, nowadays, generate personal data or use such data as input, and this is not different for EU institutions and bodies. This means that *effective protection of personal data*, as a fundamental value underlying EU policies, should be seen as a *condition for their success*. This message has been received well and will continue to drive activities in the near future.

Supervision

A first emphasis has been put on the development of the network of *Data Protection Officers* in all institutions and bodies. In November 2005, a position paper was issued on the role of DPOs in ensuring effective compliance with Regulation 45/2001. The position paper was sent to the heads of the EU administration and underlined the role of the DPO as a strategic partner for institutions and bodies in ensuring compliance.

A major second emphasis has been on the *prior checking* of processing operations which are likely to present specific risks for data subjects, as mentioned in Article 27 of the Regulation. Although this task was typically designed to deal with new processing operations, most prior checks have been 'ex post' prior checks, due to the fact that many existing systems would have qualified for prior checking, had the EDPS been available at the time of their entering into operation. In most cases, opinions recommended substantial improvements to ensure full compliance. Opinions are published at the EDPS website and their follow up is monitored.

A third emphasis has been on the handling of *complaints*. However in 2005, only a few complaints were declared admissible. In practice, a large majority of complaints, such as complaints about national data protection, do not raise issues for which the EDPS is competent. In such cases, the complainant is informed in a general way and, if possible, advised on a more appropriate alternative. With respect to the handling of complaints within my competence, I have contacted the European Ombudsman to examine a potential scope for collaboration in the near future.

Considerable efforts have also been invested in the elaboration of a background paper on *public access to documents and data protection*, issued in July 2005 with a view to promote a balanced approach to both fundamental interests. Special attention has also been given to supervision of *EURODAC*—a large system

with fingerprints of asylum seekers—which requires a close cooperation with supervisory authorities in the Member States.

Consultation

A first priority in this area has been the definition of a *policy on the role of the EDPS* as an advisor to the Community institutions on proposals for legislation and related documents. A policy paper was issued in March 2005, which emphasizes that the advisory task has a wide scope and deals with all proposals for legislation with an impact on the protection of personal data. The policy paper also sets out the substantive approach which we intend to take to such proposals for legislation and my role in the different stages of the legislative process. A formal opinion is always published, often presented in a committee of the Parliament, or the competent working party of the Council, and systematically followed on its way through the legislative process. The Commission has reacted very positively to this policy.

In 2005, I have issued six formal *opinions* which reflect the relevant subjects on the policy agenda of the Commission, the Parliament and the Council. Important opinions related to the exchange of personal data in the third pillar, the development of EU wide information systems—a Visa Information System (VIS) and a second generation Schengen Information System (SIS II)—and the highly controversial subject of the retention of traffic data on electronic communications for access by law enforcement authorities.

I have also, for the first time, made use of the possibility to *intervene in cases before the Court of Justice* which raise important questions of data protection. The Court granted a request to intervene in two cases on the transfer of PNR-data on airline passengers to the United States, in support of the conclusions of the Parliament. Both written and oral observations have been presented, and we are now looking forward to a decision of the Court.

The EDPS has a special task in *monitoring new developments* that have an impact on the protection of personal data. I have therefore made an initial evaluation of new technological trends—e.g. RFID, Ambiant intelligence environments, Identity management systems, biometrics—and developments in policy and legislation that will be followed systematically in 2006 and thereafter.

Cooperation

An important platform for cooperation with national supervisory authorities is the *Article 29 Working Party*, set up by Article 29 of Directive 95/46/EC, of which the EDPS is a full member. Some important proposals for legislation were covered by the EDPS and the Working Party in separate opinions. In these cases, I have welcomed the general support of national colleagues as well as additional comments which can lead to better data protection.

Cooperation with *supervisory bodies in the 'third pillar'* has concentrated to a large extent on the preparation of common positions with a view to the development of a highly needed framework for data protection in the 'third pillar', dealing with police and judicial cooperation in criminal matters. More specifically, discussions have taken place about a new system of supervision with regard to the new generation Schengen Information System (SIS II), which will build on a close cooperation between national supervisory authorities and the EDPS.

In September 2005, in cooperation with Council of Europe and OECD, I have hosted a workshop in Geneva on data protection in *international organisations*. There is room for improvement in this area and other initiatives are therefore likely to follow.

Other areas

The EDPS has also invested in development of an *information strategy* and enhancement of *information and communication tools*. An information campaign for EU institutions and bodies and all Member States, with brochures in all Community languages, was followed by the introduction of a press service and a regular newsletter, and will soon be completed by the introduction of a new website, as the most important tool of communication.

Major attention has been given to the development of *human resources*. Important results have been reached, both in recruitment and in special programs for stages and secondment of national experts. The actual size of the organisation in 2006 will be slightly higher than 25 full time positions.

Finally, it is difficult to overstate the importance of the *administrative agreement*, concluded in 2004 with the Commission, the Parliament and the Council, which has enabled us to benefit from outside support where appropriate, and to invest most resources in primary activities.

Concluding remarks

We have started in January 2004, but most of the first year was used to make the first steps in the 'building of a new institution' and the development of its strategic roles at Community level, to monitor and ensure the application of legal safeguards for the protection of personal data. Most staff joined the EDPS only at the end of 2004.

After two years, the independent authority is shaping up well, and it has also been able to position itself as a new authoritative and visible player in a highly relevant area. This is partly due to many persons in different institutions and bodies with whom we closely cooperate and who are responsible for the way in which data protection is 'delivered' in practice, but most of all to the members of the staff who take part in our mission, and continue to make a major difference in its results.

A few weeks from now, I shall be presenting my second annual report, and please allow me to refer to that report and to website www.edps.eu.int for further details.

7

Directive 95/46 in the French-Speaking World

Emmanuel de Givry
Commissioner of the CNIL [French Data Protection Authority]

The impact of the 1995 directive in the French-speaking world is the result first of the nature of the document. Its objective is harmonization of national legislations, in a field affecting human rights. The convergence of legislations in this regard may only be by way of increasing the protection given to individuals. Implementation of the directive in no case may result in a decrease in the existing level of protection in a Member State.

The consequence of this principle was that the directive benefited from all advances in the various European countries, and all legislations have emerged from the process stronger than they were.

This also was the case in France. The so-called "Informatics and Freedoms" law of 1978, the third in the world after Hesse Land and Sweden, at the time was considered to be very protective. The French Constitutional Court in 1992 recognized it as being *supra-legislative*. This means that any other law must conform to its principles protecting individual freedom. The Court also has held that privacy is a protected constitutional right.

From that point forward, the first effect of the directive, in France, was to provoke extended discussion, taking into account the huge increase in information processing, concentrating on the question of effectiveness of the measures applying

the principles. The French law, extensively amended in August 2004, has taken advantage of all options available under the directive to change its approach to personal data protection. These matters of modernization and improvement of the French law are what I will first discuss.

The second aspect of the impact of the directive in the French-speaking world relates to countries outside of the European Union. It is explained by matters of an economic, political and legal nature, and the efforts of French authorities to cooperate with those countries. These are the questions I will deal with second, in light of what is currently happening in the world.

Plan:

I. Implementation of the directive in France
II. The dynamic created by the directive in French-speaking countries

Implementation of the directive in France

General presentation of the French law

a) *Scope of application and principles*

The 1995 directive applies to both the public and private sectors, within the scope of community jurisdiction. The French personal data protection law has an even broader scope of application, since it also covers activities related to public security, defence, and security of the State (with the necessary adaptations).

Under the directive, the French law is applied both to automated processing and to manual files, with the exception of processing undertaken in the exercise of exclusively personal or domestic activities.

In order to assure a high level of protection, the definition of the essential concepts by the directive, and by French law, is as broad as possible, and allows inclusion of voices and images of individuals, as well as the later appearing *RFID*. The definition of data processing allows inclusion of the nanotechnologies and the Internet.

The directive has harmonized the principles of lawfulness of processing in all European countries. As a reminder, these are:

— the principle of responsibility of the persons that engage in processing;
— the principal of transparency (which implies knowledge of the existence of processing, and the possibility for individuals to know what data are recorded in the processing);

— the principle of a determined and lawful purpose;
— the principle of proportionality between the data recorded and the retention period;
— the principle of security and confidentiality of the data;
— the principle of consent of the data subject, except in specified cases.

The first article of the "Informatics and Freedom" law, unchanged since the beginning, is the pillar for the protection principles, and underlies the actions of the supervisory authority:

> Informatics must serve every citizen. Its development must be undertaken within the framework of international cooperation. It must not jeopardize human identity, human rights, the privacy of individuals, or individual or public freedoms.

b) *The National Commission on Informatics and Freedom and its missions*

The uniqueness of the European personal data protection system lies in the institution of supervisory authorities, independent and with effective powers. The supposition is double: the actors, public and economic, cannot at the same time be judges and parties. Such agencies are capable of adapting to changing situations, especially to the fact of technological evolution.

The National Commission on Informatics and Freedom (CNIL) is the French supervisory authority, created by the law of 6 January 1978. It is a single agency with national jurisdiction, which has a very specific charter. In fact, it was the first French "independent administrative authority": an institution of the State, but not subject to the hierarchical authority of a minister.

The independence of the CNIL also is reflected by its composition and the manner of appointing its members. It is a collegial body comprised of 17 members of diverse backgrounds. It elects a chairman and vice chairman from among its members. It freely establishes its internal regulations.

The general mission of the CNIL is to oversee respect for the rights and freedom of individuals, satisfying itself that processing complies with the requirements of law. Evolutions of technologies and the consequences they may have on the functioning of society, human rights and privacy must be very closely watched.

In addition to its traditional activities, which are those of any supervisory authority (providing information and advice to data subjects, controllers and the public authorities, registration of file notices, handling of complaints and monitoring processing, etc.), the CNIL in 2004 inherited new functions, such as the

possibility of issuing opinions regarding professional rules, and granting certifications of products or processes.[1] The law henceforth requires that the commission advise the government regarding matters of international cooperation, and cooperate with the other authorities in the field of personal data protection.

In performing its missions, the supervisory authority often must seek balance between divergent or even contradictory interests. This is the case of reconciliation of security demands, for example combating terrorism, with individual rights and freedoms. It is also necessary to balance the interests related to transparency and access to information with those related to protection of privacy. The CNIL, as in several other European countries, in this regard advocates complete removal of names and addresses of data subjects from judicial decisions placed on the Internet.

The principal innovations in the 2004 law

The law of 6 August 2004 has profoundly changed the French approach to supervision of data processing. It has used all options available under the directive to alleviate and simplify notice procedures, compensated for by greater supervision of the most dangerous processing. Similarly, there has been a rebalancing as between *prior control* of processing, which always has been the CNIL's preferred mode of operation, and *after the fact control*, particularly based on a new power of administrative sanction.

a) *Relief regarding prior proceedings (notification) and the creation of the "personal data protector"*

Under the directive, processing that involves personal data must be notified to the supervisory authority prior to being undertaken. The 2004 law has eliminated the distinction between the public and private sectors. Notification now is a common requirement. In this regard, the commission's supervision is limited to verifying that the notification meets the formal requirements, and registering it. The CNIL can simplify notification for certain processing considered to be of little danger, strictly limiting it by regulations issued by it.[2]

Going even further in simplification, the law contemplates cases in which no formality is required (in particular legal registers used only for informing the public

[1] The power to certify products and processes, which is not expressly contemplated by the directive, exists only in the German *land* of Schleswig-Holstein.

[2] The CNIL to date has issued 50 of these "simplified rules".

and certain processing undertaken by associations). It also gives the CNIL authority to grant exemptions from notification for such processing as does not present risks to rights and freedoms. The French authority already has used this power on several occasions (for example regarding paying personnel, and a short time ago regarding blogs or websites created by private persons).

Another essential innovation of the amended French law is the creation of "data protectors" (called "informatics and freedoms correspondents" in France). The system, contemplated on an optional basis by the directive, comes to us from Germany, and has also been adopted by Holland and Sweden. A company or agency that appoints a "protector" is relieved of compliance with notice procedures, except in those cases in which authorization is required. This means that with respect to the applicable matters the action of the correspondent becomes that of the commission.

The functions of the correspondent are essentially maintaining the list of processing undertaken by the company, responding to requests from data subjects (in particular regarding the exercise of the rights of access, rectification and opposition), and in general advising the controller regarding protection of personal data and compliance with the law.

Since the end of 2005, when the correspondent mechanism became operational, some 170 organizations have appointed one.

b) *Strengthening prior control of "risky" processing*

Relief regarding prior proceedings for most processing allows a refocus with respect to the processing presented, by reason of the nature of the data recorded or the purpose of the processing, on specific risks to the rights and freedoms of individuals. True prior control implies verification of both the lawfulness of the processing and the contemplated guarantees. This in particular involves: entry and processing of "sensitive" data, of genetic or biometric data, the processing of data regarding violations or convictions, processing that may result in exclusion from a right or contract, interconnections of files that have different purposes, etc. The CNIL's control of such processing consists of granting or denying an authorization binding on the controllers.

The French authority already has issued several decisions authorizing or rejecting biometric control devices for access to certain premises, regarding the fight against Internet falsification (*peer-to-peer* networks), and professional alert devices (the famous *ethics lines* implemented in application of the Sarbanes-Oxley Act).

Regarding biometric control devices, the CNIL through its decisions has developed some assessment criteria for authorization or rejection of such processing.

The first criterion refers to the kind of biometric technique used. The commission authorizes processing using so-called "non-tracking" technologies (for example the shape of the hand), because they do not involve a risk of use for other purposes without knowledge of the data subject. By contrast, it is very strict regarding the use of "tracking" biometric techniques (fingerprints, facial recognition, etc.), for which a second assessment criterion is taken into account. The CNIL authorizes devices based on recording the tracked information on a separate medium (card), if security objectives so justify, or if the device is used voluntarily (with the difficulty of assuring the free and informed consent of data subjects). The CNIL allows data to be entered in a database only if strong security requirements are in play (airports, nuclear plants, etc.).

Finally, the directive has confirmed that the recognized protection level must be assured in cases of international transfers. For this reason, processing that contemplates transfer of data to countries that do not provide a sufficient level of protection also must be authorized. In this context the commission verifies both the lawfulness of the transfer and the safeguards presented by the contract clauses or internal rules applicable thereto.

The dynamic created by the directive in French-speaking countries

Origins of the dynamic

The dynamic created by the directive in French-speaking countries outside of the European Union was immediate in an industrialized country like the province of Quebec. After adoption of the directive, it was the first State to extend its *law on protection of personal information*, to the private sector. It initially had been applied only to the public sector. At the federal level, Canada adopted this approach shortly thereafter. The adequate level of its law was recognized by a 2001 European Commission decision.

Another dynamic, more recent, relates to the French-speaking countries in the Southern Hemisphere. It is explained by economic, political and legal factors.

The first factor is related to the very rapid growth of information and communications technologies (in particular the Internet and mobile telephones) in the developing countries.

The second factor relates to the activities of the International Organization of the French-Speaking World (OIF). Fifty-three States from all continents are members. Initially established on the basis of a common language, French, this

organization increasingly is concentrating on common values related to democracy and human rights. Thus it naturally has considered the new right of personal data protection.

The French "Informatics and Freedoms" law and the 1995 directive in this context are taken to be fundamental laws. An advantage of the directive is that it may be applied to various legal contexts, since it was prepared in a region of the world where various legal systems coexist.

Adopting a law of this kind also is consistent with the wishes of companies that the country where they are located be recognized as ensuring an adequate level of protection. This can provide a favourable framework for international interchange, especially with the French-speaking countries in the Northern Hemisphere, France, Canada and Belgium.

Current developments

a) *The beginnings*

The international conference of data protection authorities organized by the CNIL in 2001 was an opportunity to invite people from the African continent to share their experiences (such as dissemination of the electoral register via the Internet, the national identity document database, the question of medical secrecy in combating AIDS, etc.). One year later cooperation was established with the Ministry of Human Rights in Burkina Faso. It was the first country on the continent to adopt legislation in the field of personal data protection, in 2004.

b) *The political impetus of the Ouagadougou Declaration*

Following the example of its Spanish counterpart, the CNIL suggested to the French government that it encourage actions of the Member States of the International Organization of the French-Speaking World in developing data protection rules. At the organization's summit in Ouagadougou in November 2004, the chapter of the final declaration dedicated to human rights ended with recognition of a new right, that of personal data protection, including the principle of an independent authority.

The heads of state and government at the meeting accepted "giving particular attention to the protection of the fundamental freedoms and rights of individuals, especially their privacy, in the area of use of databases or processing of personal data." They have called for "the creation or consolidation of rules guaranteeing such protection" and supported "international cooperation among the independent authorities responsible for supervising respect for these rules in each country."

c) Pre *and* post-*legislative action plans*

Twelve of the 53 States that are members of the International Organization of the French-Speaking World have data protection legislation and an independent authority responsible for it. All but one are states in the Northern Hemisphere. Actions currently being taken in this context are of two kinds: pre-legislative and post-legislative, within a multilateral or bilateral framework.

In the *pre*-legislative phase, the CNIL is involved in awareness activities, within the framework of meetings of the OIF with those responsible for the State's legal institutions (higher courts, agencies responsible for human rights, attorneys, independent authorities and associations, etc.). These relationships also offer opportunities to identify spokesmen and make information available to them, in a bilateral framework. When a legislative initiative is decided upon, the CNIL may be invited to participate in preparatory seminars or review the proposed law.

The main difficulties encountered relate to creation of the authority, and are of a financial (resources) and political (the question of independence of the political authority) nature. One route to solution of the latter problem is a pluralistic makeup of the body.

Regarding the *post*-legislative phase, the chairman of the CNIL, Alex Türk, and the chairman of the Monaco authority have decided to consult with their counterparts regarding the possibility of creating an association of the independent French-speaking authorities. The intent would be to create:

— a vehicle for cooperation and interchange regarding good practices;
— a centre for expert advice available to the States during pre-legislative phases;
— a base for initiative on a global basis, in particular for implementation of the Montreux resolution.

This association may be born in 2007 on the occasion of a French-speaking conference prior to the International Conference of data protection authorities.

Conclusions

The CNIL of course is available to those who wish to take advantage of its experience during pre-legislative processes. As always, it will be interested in meeting with representatives of new authorities seeking interchange regarding good practices, either by way of visits or of course during the international conference.

The facts seem to confirm an intuition: although Internet technology is not European, Internet law may become so. In fact the European laws regarding information technologies are a reference source for their regulation, favouring their harmonious development, not only in European countries but also in other parts of the world. This involves not only the law regarding data protection in general, but also the complementary law of 2002 regarding electronic communications and privacy, the so-called "e-commerce" directive and the law regarding electronic signatures.

It is an honour for Europe to share the harmonization that has been achieved among the various legal systems; it also is a great responsibility. Therefore some may feel that on a worldwide level, in the continuations of the World Summit on the Information Society, where such matters are considered, Europe need hear nothing further regarding data protection. It potentially has natural allies, the other countries that have committed to develop it, such as the Ibero-American countries and those in the French-speaking World (a total of 100 countries, half of the planet). It would be necessary to confirm their conviction with them, and take initiative supporting the regional and national efforts, as now promoted by the International Conference, to prepare an international treaty.

It is not sufficient to have "a good treaty or a good law" during a period marked by fears of an international nature. Some are in favour of adoption of legislation that largely repeals the basic principles of data protection. In this context, as some speakers have already emphasized, the voice of independent authorities is essential, to contribute at least to encouraging public debate, based on propositions clearly establishing the appropriate balance between security and freedom.

8

Data Protection in Canada: Adaptation, Similarity and Information Policy

Esther Mitjans
Director of the Data Protection Agency of Catalonia

Introduction

In this 21st century, Canada's problems are those of a society with a highly developed economy, with the challenges presented by the global economy to maintenance of the democratic standards it espouses. Canada is a member of the G-7 and a leader in multilateralism in international policy. Behind this is the debated progressive constitutional dissociation of the United Kingdom. Multiculturalism has added a new face to the well-known differences between English-speaking Canadians and the Quebecois.

The fact that the 1982 Canadian Constitution included a Charter of Rights and Freedoms was much debated at the time. Pierre Trudeau's determination to include it required him to introduce the "notwithstanding" clause to secure acceptance of the provinces. This clause permits them to disassociate themselves from the Charter regarding certain matters.

Also, the Charter has a clause limiting the rights.

In comparative constitutional law there are three methods for limiting rights. One method is that of the US Constitution, which establishes the rights and leaves it to the courts to consider the limits. Another is that of the European Convention,

pursuant to which each right has stated limits. The third is that of the Canadian Constitution, which contains a limiting clause containing a balancing test that is applicable when other rights or values must be taken into account. This latter method is applied in international documents (universal and European declarations of human rights) and in countries with a common-law tradition such as, as we have stated and among others, Canada. Contributing to this, in addition to the influence of international law, is the tension between the principle of parliamentary sovereignty and the guarantee of rights as an integral part of the highest law. In Canada this modifies relationships between the legislature and the courts, limiting the classical parliamentary supremacy in the British model.

The Canadian Supreme Court often refers not only to the case law of the US Supreme Court, but also to that of the European Court of Human Rights. Nevertheless, the clause in the Canadian Charter limiting the enumerated rights is a more generic limitation than the specific limitations in the European Convention.

This technique of establishing a balancing test for rights and values in the constitutional text itself was used in an attempt to include the right of privacy and the right of access to information in the Charlottetown constitutional reform agreement. The failure of this attempt to reform the Constitution prevented these rights from appearing in the Charter of Rights and Freedoms, despite their later recognition by the courts.

Nevertheless, before the Constitution, Canada had already adhered to the guidelines of the OECD on data protection (1980). And in 1983 it simultaneously adopted two laws, one for data protection in the public sector and the other regarding access to information, which we will address later. First we will discuss the future impact of European Directive 95/46/EC and, in this regard, the provincial jurisdiction regarding data protection.

Adaptation to the European Directive

The development of the new technologies regarding personal data protection and the need to adapt to the European Directive led Canada in 2000 to adopt the Loi sur la Protection des Reinsegnements Personnels et des Documents Electroniques (LPRPDE), which applies to the private sector. We must not forget that the referenced Canadian Charter does not apply among private persons. The government must be one of the parties in order to be able invoke the Charter. And the data protection legislation, as we have said, also relates only to the public sector.

In turn, as we will see later, Quebec has been the first country in North America to promulgate laws for protection of personal data both in the public and private sectors.

Canada followed it with the LPRPDE [Loi sur la Protection des Reinsegnements Personnels et Documents Electroniques]. They are the only North American countries that have legislation of general application, by contrast with the United States, whose legislation applies by sector and is left to self-regulation in the private area (with an attempt to solve that by means of the "Safe Harbour" agreement).

The European regulation is exported by means of the directive, allowing the interchange of data and benefiting international trade. The directive, applicable in the public and private sectors, prohibits transfers of personal data to third countries that do not provide an adequate level of protection. The adaptation requires effective application of the rules.[1]

The 2001 Decision of the European Commission pursuant to the directive recognized the adaptation of Canadian legislation, through promulgation of the LPRPDE.

The LPRPDE, as we have said, applies to the private sector (the protection of data of citizens processed by federal institutions had already been regulated, as we have stated) and to federal undertakings, both in their business relationships and as regards their own employees.

The law was inspired by the 10 principles in the model code for protection of personal data adopted by the Canadian Standardization Association (ACNOR), which are added in Annex I to the Law. These principles, nonetheless, have been interpreted by some more as recommendations than as obligations.

The basic similarity of the provincial laws

If an essentially similar provincial law is applied in a province, it is exempt from application of the LPRPD, thus respecting the jurisdiction of the provinces. It has been recognized that Quebec, Alberta and British Columbia are exempt from application of the federal law.

---

[1] Duaso, Rosario. " El derecho a la protección de los datos personales en el ámbito privado en la legislación federal canadiense y quebequense" in Derechos y Libertades en Canadá, Mitjans, E. (edit.) and Castellá, J. M. (coord.). Edit. Atelier, Barcelona, 2005, p. 361.

"Basically similar," despite its apparent vagueness, implies respecting the basic principles of the LPRPD, set forth in its Annex I, the existence of an independent authority and the possibility of complaining if the data protection right is violated.[2]

The Charte des droits et libertés de la personne de Quebec is of particular interest, as it covers the public and private sectors, applying not only to relationships with the state but also among private persons.[3] The 1991 Quebec Civil Code announced the protection of privacy. It was implemented in 1994 in the first North American law regulating the private sector within the territory of Quebec. Interprovincial and international processing, and the activities of a federal undertaking within Quebec, also are governed by the LPRPDE.

Information policy in Canada

Data protection is just one aspect of a broader problem, that of distribution or dissemination of information within a specific society. This new perspective has been required by the new technologies, which demand redefinition of the right of privacy from the right to be left alone to the right to control use of information legally obtained by the public authorities or private persons. The accumulation of data by these authorities using the new technologies requires measures to balance or reduce the disparity existing as regards a citizen who has no knowledge of the data about him that is contained in the files.

Paradoxically, the legislation has come to ensure opacity in the private sphere by establishing transparency for the actions of public and private institutions.[4] The intention is for data controllers to be ever more subject to supervision. For that purpose visibility and transparency is required of them. It is a matter of balancing the citizen's lack of defence. This has now become a condition or criterion for lawful exercise of public authority. The right to be informed does not compromise these actions. The opposite is true; it increases their credibility.

---

[2] Duaso, Rosario. "El derecho a la protección de los datos personales en el ámbito privado en la legislación federal canadiense y quebequense" op. cit. p. 366.

[3] Benyekhlef, Karim. "Les dimensions constitutionnelles du droit a la vie privée", in Droit du public a l'information et vie privée : deux droits irréconciliables ?, Trudel, P. and Abran, F (dir), Éd. Thémis, Montreal, 1992, p. 42.

[4] Legislation and Data Protection. Proceedings of the Rome Conference. Edit. C. Diputati, Rome, 1983, cited by Mitjans, E. "Los limites a la privacidad en Canadá" in Derechos y Libertades en Canadá, Mitjans, E. (edit.) and Castellá, J. M. (coord.). Edit. Atelier, Barcelona, 2005, p. 372.

It is for this reason that, in some countries like Canada, the data protection laws have evolved together with those regulating access to public documents, even to the point of both aspects being regulated in the same law.

The information policy that exists in Canada is intended to answer the questions of under what conditions information will be given, to whom, what kind of information, and for what purpose. Based on the functions of States in information societies as social and democratic states and states of laws.

Modern states in advanced countries are seen as networks for production and interchange of information. The new technologies have changed the context. Information is not at a specific place but rather it is available on the web. The problems regarding access in large part are the conditions for access to the web. Political decisions are based in large part on the information available on the web.

As public bodies confer responsibility on the private sector that heretofore was assumed by the state, it is difficult to identify the boundaries between what is public and what is private. The outsourcing of public services expands the concept of "public." But there cannot be a loss of control by the citizens.

Freedom of expression and freedom of the press allowing criticism of governmental actions are not sufficient. It is essential to have the necessary information to understand the motives for governmental decisions. The technological environment allows greater transparency in justification of these decisions. The State is an essential source of information for the conduct of many activities within society. To the point that almost 50% of requests for governmental information come from the private sector.

Companies benefit from this information by knowing the government's needs when they are going to contract with it (thus it is not surprising that the World Bank, the IMF, recommends that countries regulate access to information).[5]

State activities and services on the web allow us to require the state to make any document that is not subject to a special and justified reservation to be made available on the Internet. This would be a requirement of the State as a democratic State.

As a state of laws, it must give the citizens the right to information self-determination and the right to privacy. But it is not the classical conflict between the

[5] Mcdonell, Roderick in "Access to Information—the Commercial Side" in Development Outreach. Putting knowledge to work for development, March, 2003,
http://www.worldbank.org/wbi/governance/journalism/resources.html

two rights, pursuant to which the citizens' right to information limits the privacy of those that are newsworthy. Rather it is how this privacy may be better assured by means of information regarding the actions of public authorities.

Canadian regulation of access to information and data protection

The thinking underlying Canadian legislation thus promotes the concept of privacy in which what is important is how movement of information is managed. Otherwise stated, how the appropriate persons obtain the appropriate information for the appropriate purposes. From this point of view, as has been indicated, the effort is to relate two rights, the citizens' right to information and the right to protection of their personal data.

The access to information obtained through normal communications media (newspapers, television, the Internet) is not sufficient. It is necessary to establish specific access mechanisms, because the actions of these authorities are not easily known. In addition to this opacity, we know that these authorities accumulate large amounts of personal data. The public authorities, as the social state or protector, need this data to implement their social policies and maintain public order.

Of special importance in the set of citizens' rights, these two rights, that of access to information and that of privacy, as we have said, are closely related in Canadian legislation. Indeed defence of these rights is attributed to a single supervisory authority in the provinces.

Their importance explains why they are regulated by quasi-constitutional Canadian laws (they derogate laws that are not compatible with them) and their complementary nature explains why, in Quebec, both matters are regulated by the same law ("Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels"). They were promulgated in Canada at the same time at the beginning of the 1980s. The "loi sur la protection des renseignements personnels" and the "loi sur l'accès à l'information." They are considered to be two sides of the same coin. The latter gives the public access to information. The other gives individuals the right to access information about them.

On the other hand, some maintain that the two laws specify their own fields of application, with opposing content, to the extent one offers information and the other limits it. But others conclude that the general right to access public documents

is extended, in the case of personal data, by the right to know the content of the files containing it and access them. In this sense, protection of privacy and state interests are more coherent and complementary than contradictory.[6] The general right to access documents held by the government is expanded, in the case of personal data, by the right to know of the existence of the files containing these data. Knowledge of the existence of the document is the necessary condition for exercise of the right of access.[7]

The Supreme Court of Canada recognizes primacy of the right to privacy in requests for access to public documents**.** There also is a thread in case law that that clearly subordinates privacy to freedom of information. This thread rejects what would be a veto right regarding decisions to inform the public upon assertion of violation of the right of privacy.

In short, in Canada the circumstances under which the data are collected and processed, and the information is distributed, are taken into account. Personal data cannot simply be treated as property, without more. Rather they must be considered within the context of global movement of information within the society, for the purpose of avoiding monopolies of information destabilizing the decision-making processes in a democratic society.

Current problems

Within these reflections one must, nonetheless, include the current controversy in Canada regarding attempts to combine the two functions (data protection and access to information) in a single supervisory authority at the federal level. As we have said, such integration exists in the provinces.

This *integration* has been roundly criticized by prestigious defenders of both information (Rubin) and data protection (Bennett).

It is reported that the information access legislation is encountering significant resistance of the Ottawa bureaucracy. The secrecy and frequent refusal to render accounts lead to the fear that, by means of this integration, it is intended to restructure jurisdiction over information in order to make it more docile and complacent as regards the actions of the government.

---

[6] Lyette, Doré, "La legislation canadiense en matière d'accés a l'information et de protection des reinsegnements personnels a 20 ou..la jeunese de coeur.. " in Developpements récents en droit de l'accès á l'information. Ed. Yvon Blais, Montreal, 2002, pp.142-143.

[7] Trudel, Pierre. "L'accès aux documents publics: des ajustements pour assurer la trasparence de l'Estat en réseaux" in Developpements récents en droit de l'accès á l'information, op cit. p. 55.

In addition it is argued that integration in a single authority would reduce the capacity to supervise the ever more powerful private sector. And also that it would limit the defence of privacy against the challenges on an international level presented in the name of combating terrorism.

Finally, this leads us to another of Canada's problems, as a country bordering on the United States.

One of the priorities of the Ministry of Foreign Affairs and Commerce of Canada is how to reconcile post 11-S *security* with the rights of its citizens.

The need to protect the intense cross-border trade with the US, which is crucial to Canada, requires seeking mechanisms to avoid an effect on the personal data of Canadians by United States antiterrorist legislation (the Patriot Act) (The Information Commissioner of British Columbia has consulted experts to decide whether it is necessary to limit disclosure of medical data of medical companies with owners from both countries).

If Canada does not accept the security measures proposed by its neighbouring country for its own border points, ports and airports, control will be transferred to the US border, which will jeopardize trade. There are many companies that work on both sides of the border.

To give us an idea of the volume of these commercial relationships, few years ago a Canadian international trade expert told me in Ottawa that trade between Canada and Spain over the course of one year is equivalent to trade in a single day between Canada and the US.

Fortunately, over recent years the situation has been changing as regards our country, through companies such as Cepsa, Bombardier, but also Seagram, Nortel Networks and Ferrovial, etc.

In any event, whatever the trade between Canada and Spain, what is evident is that the obstacle will not be Canadian data protection legislation, given its acknowledged adaptation to European legislation.

Part III

DATA PROTECTION AND ECONOMIC ACTIVITY: BINDING CORPORATE RULES

9

What is the *Raison d'etre* of the Binding Corporate Rules?

Jacob Kohstamm
Chairman of The Dutch Data Protection Authority

Transfer of personal data outside the European Union is subject to data protection legislation. The basic rule is that data may not be transferred to a country outside the European Union unless there is adequate protection for the data that are transferred. The rationale behind this is that data subjects should continue to benefit from the protection they have under EU law and that they should also continue to be able to exercise their rights. This protection can be provided by the rules of the third country itself. In case there is no regulated protection in the third country, the data controller transferring the data will often have to provide adequate safeguards for the transfer to make up for the lack of protection for the personal data in the third country. Such safeguards traditionally follow from contractual clauses which are concluded between the controller in the EU who exports the data, and the recipient or recipients outside the EU. Each member state implemented these rules, laid down in 95/46/EC Directive on data protection, in its own manner. Although the basic rule is the same everywhere, there are in practice both procedural and material differences between Member States in the evaluation of the applications for transfer of personal data. These differences concern, for example, the amount of information that is to be provided, what forms should be filled, etc. For example in two Member States, NL and Belgium, a

permit to transfer data to third countries is granted by the Minister of Justice—after advice is obtained from the data protection authority—in other Member States the data protection authority is qualified to give authorizations. Another striking difference is the difference in handling of requests for transfer when the controller uses standard contractual clauses. In some Member States a permit or authorization is still required, in others an authorization or permit is no longer necessary.

In the Netherlands, since the implementation of the Dutch Data Protection Act in 2001 the Dutch DPA (CBP) advises the Minister of Justice on the request for a permit to transfer data to third countries, however the Minister of Justice has discretionary power to grant or withhold the permit regardless of the nature of the advice of the Dutch DPA.

Some figures to give you an idea of the number of applications for transfer permits received so far: in total 96 requests for a permit to transfer data have been received. Thereof 61 advices regarding the request for a permit have been presented to the Minister of Justice. Twenty requests for a permit have been withdrawn or ceased by the applicants. Another 15 requests are pending, of which 3 BCRs whereby the Dutch DPA is the lead authority and 2 BCRs are handled in the framework of the co-ordination procedure.[1] I will get back to this.

Most of these 94 requests were made on the basis of contractual solutions —agreements concluded between the data importer and the data exporter— which are assessed by us in light of the principles set out by documents issued by the Article 29 Working Party and especially the Commission decisions on standard contractual clauses. These contractual solutions work very well within enterprises that transfer either a limited set of data or that send data to a limited set of controllers or processors in third countries.

Problems arose in the Netherlands when a multinational company requested a permit to transfer personnel data to 2500 affiliates in 140 countries. After several discussions with the applicant a contractual solution was reached. The applicant appointed 140 country managers as controllers for the processing of data by all affiliates established in their respective territories. This required the conclusion of 140 agreements between the data importers and the data exporter. Luckily, data were exported outside the EU only via the Dutch headquarters.[2] As you understand, this was a very time consuming activity and the permit for

---

[1] Situation per 16 March 2006.

[2] See: http://www.cbpweb.nl/documenten/uit_z2002-1426.stm?refer=true&refurl=http%3A//www.cbpweb.nl/themadossiers/th_doo_praktijk.shtml&theme=green

transfer of data only applied to this specific data transfer. The situation would become difficult to manage in case all transfers within the global company would have to be covered by the contracts. A web of hundreds of contracts would be the end-result.

Not only Dutch multinationals face this problem, multinationals established in other Member States encounter similar problems. The whole situation is even more complicated when multinationals wish to transfer data from various or all Member States to third countries. This is due to the procedural and material differences in implementation of the European Directive in national legislation. Multinationals experience this whole situation as unnecessarily burdensome, and are of the opinion that contractual solutions do not take into consideration that some transfers take place worldwide. Apart from the procedural complexities of managing applications in sometimes 10 or more countries, the situation becomes even more complex when different countries apply differing material rules to exactly the same processing. In other words: the lack of flexibility of contractual mechanisms became ever more pertinent.

Development of the BCRs

Throughout Europe, faced with the administrative burdens of handling the transfers of personal data and in an era of globalisation, multinational companies started discussions with DPAs to explore the possibility of a new legally binding arrangement. This new legally binding arrangement would on the one hand have to ensure data protection throughout the company whilst also better meet the daily business realities of global companies. Could adequate safeguards also be adduced by non-contractual means, for example by means of codes of conduct? This lead to the development of Binding Corporate Rules: codes of conduct for international data transfers within multinationals. The idea behind this is that companies will implement the data protection rules in their global organisation, document this, and ensure compliance through their corporate governance mechanisms. Rather than relying on contracts only, the focus of BCRs is thus on the practical and effective application of data protection rules within organisations; companies must show how and prove that the general principles of the BCR are adhered to at all levels of the organisations.

This approach would be in line with the work program of the European Commission after its first evaluation of the directive in 2003. The Commission then concluded that it favoured not only high, but also effective standards of data

protection, and a more consistent application of the directive across the EU, and the alleviation of any unnecessary administrative burdens. With BCRs, three of the objectives of the Commission in this context are met:

1. reduction of divergences in Member States practice, helped by Article 29 Working Party;
2. more flexible arrangements for transfers of personal data to third countries, together with a clearer and more uniform interpretation of the rules;
3. promotion of self-regulatory approaches and in particular codes of conduct that can contribute to the free movement of data.

In June 2003, after lengthy discussions, a document on Binding Corporate Rules was adopted by the Article 29 Working Party. In this document the most important elements of a code of conduct aimed at guaranteeing an adequate level of protection for internal exchanges of personal data within the multinational, irrespective of their place of business, are described. Emphasis is put on *real* and *effective* protection, the *de facto* compliance to the code of conduct is regarded as very important, however these commitments also need to be binding in European law or enforceable before European courts.

The advantage of this approach is that it is more closely aligned with the business realities of companies. The emphasis shifts to practical compliance, which will result in higher data protection standards rather than imposing the burden of complex administrative procedures to conclude contracts. Companies can integrate data protection into their regular global compliance programs, like they have on ethics, environmental issues or financial integrity.

However, a new administrative complexity showed up at the horizon; if global companies use one and the same instrument to regulate data processing in their organisations, this one instrument should be approved in the various EU Member States. On the basis of the current applicable law rules, all authorities individually have to authorise the code. This raised questions on the feasibility of one code for all data transfers. If each involved authority poses questions on the wording, the issues addressed in the code and so on, without a point of co-ordination to streamline the process, the adoption of a single code would be—at least—time-consuming.

The companies would only be willing to invest resources in developing BCRs as long as enough data protection authorities were willing to actually accept and authorise the use of the BCR and, of equal importance, if one data protection authority would serve as a co-ordinator.

Again, the differences in implementation of the directive in national legislation and the general differences in legal systems throughout Europe challenged the data protection authorities to communicate and find solutions.

The data protection authorities recognized the importance of the BCRs and —after a public hearing in November 2004 organised by the Dutch DPA—in April 2005 two Working Party documents were adopted to facilitate the assessment of proposed BCRs.[3] The authorities agreed on a so-called co-operation procedure to co-ordinate the handling of the BCRs, and issued a model checklist that each company should fill in when filing a request in several EU Member States. It was decided that one DPA should act as the *lead authority*, on the basis of certain criteria such as the place of establishment of the company's (EU) headquarters and what information should at least be provided to the lead authority. The lead authority starts discussions on the draft code with the applicant and acts as a liaison between the company and the other participating DPAs. At the moment one code has been put forward and reached its final stage: the consolidated final draft of the GE code whereby the UK Commissioner acted as the lead DPA.

Complicating factors

There are two complicating factors in handling the BCR applications:

First there is the imbalance in establishments of European headquarters of multinationals.

Starting point to decide which DPA acts as lead DPA is the place of business of the headquarters in Europe, even though this is chosen as an objective criterion to prevent applicants from *shopping*, there is a consequence. It appears that more multinationals are established in the northern part of Europe. Most BCR applications are handled in this area. The authorities that currently act as lead DPAs are the UK Commissioner for GE, the Dutch DPA for the BCR of Philips, and more queries have been made.

Secondly, there is a difference in the assessment of instruments of self-regulation versus legislation. This is a cultural issue: the northern European countries are, due to their legal system, more oriented on the use of self-regulatory instruments to achieve certain goals. In the south there is a history whereby clear obligations and prohibitions are put forward by legislation. In the Netherlands, excellent self-regulation comes close to legislation. There is no normative difference

[3] Working Document setting forth a co-operation procedure for issuing common opinions on adequate safeguards resulting from "Binding Corporate Rules" (WP107) and Working Document establishing a model checklist application for approval of Binding Corporate Rules (WP108).

between those two. If a BCR is well placed within the organisation of the applicant and internal and external bindingness are reached, it almost equals the power of legislation. Self-regulation could contribute to avoiding administrative burden on companies and can possibly contribute to the general trust that citizens have in organisations. This way self-regulation helps individuals to give their trust to businesses and government agencies, and to society as a whole. A society that is able to generate this social capital for its citizens has created an important condition for prosperity, well-being and social cohesion. Of the essence is that the self-regulation contains two elements: trust and a compliance structure to assure the binding nature of the chosen solution.

Summarizing, it may be said that there are cultural differences in assessing self-regulation versus legislation, that places of establishment of multinationals may be unequally divided, however if alleviation of administrative burdens and adequate data protection are the goal of the DPAs, BCRs seem to be the answer. It combines self-regulation and still allows DPAs to supervise the processings taking place and where necessary allows them to intervene.

Bindingness of the BCRs

As said, an element that should be present in all systems used to adduce safeguards is the binding nature of the solution, both internal (within the organization) and external (enforceability of the rules by data subjects and authorities). Binding corporate rules do not entail contractual solutions whereby the contracting parties reach an agreement on the terms of the data transfer. The BCR will be adopted by the Board of Management of a multinational and the organisation as a whole is responsible for the compliance with the rules set out in the BCR.

How can bindingness be guaranteed?

Internal Bindingness

Internal bindingness is achieved when all affiliates abide by the rules set out in the code of conduct irrespective of the applicable legislation. This can be reached by using the regular channels to impose, for example, the general business principles or safety regulations. The BCR will only be effective if its rules are put to *practice*. Members of the corporate group and the employees need to comply with the internal rules. Elements that should be addressed in the BCR are: special education programs for employees, individual and effective information of employees

and transparency on disciplinary sanctions if the BCR is circumvented. The Dutch DPA highly values availability of system documentation and audits on processings, which—if performed regularly—raise awareness on data protection issues within the organisation. I will get back to this when I discuss an issue that arose while discussing the Philips BCR.

External Bindingness

An individual needs to be able to enforce the content of the code of conduct in cases where the multinational does not voluntarily grant redress and, if necessary, to obtain compensation for damages suffered. This can be reached by either legal effects, by unilateral undertakings or contractual arrangements. The last would again be considered burdensome by multinationals and raise the question whether it makes sense to put a lot of time and effort in developing BCRs while the standard contractual clauses can also be used. In the Netherlands all three mentioned options to provide that the data subject can enforce its rights are possible. In other European countries a unilateral declaration is impossible under their legal system. This is, for example, the case in Italy. The data subject should be able to enforce compliance with the BCR both by filing a complaint before the competent data protection authority and before the competent court on EU territory. In the BCRs handled by the Dutch authority not only these two options are included, also the preliminary step to complain at the responsible party is incorporated.

Philips BCR and the issue of internal bindingness

As said previously the bindingness of the Binding Corporate Rules is essential in the realisation of effective data protection. Philips is one of the world's biggest electronic companies and has 160,000 employees in over 60 countries. Data transfers take place worldwide and on a daily basis. Contractual solutions would be time-consuming and do not guarantee compliance with privacy rules in practice.

The Philips code of conduct consists of two documents: the code itself containing the main commitments and the Privacy Rules that specify these commitments according to legal requirements. Specific privacy policies are available for consumer, HR and IT data.

In order to create adequate safeguards within the organization, to realise the internal bindingness the following issues are addressed within the privacy code and rules and have been discussed with the Dutch Data Protection Authority.

These discussions on internal bindingness lead to a three-step solution: first, a structure with dedicated officers, second, mandatory privacy impact assessments and system documentation as well as training of staff involved in data processing and third audit and performance monitoring.

An extensive *structure* has been put into place: a chief privacy officer is appointed and every Business Unit has its own privacy officers. These officers are instructed to look after compliance and handle privacy requests and complaints.

Privacy impact assessments are mandatory for each new data processing project and for each functional change to an existing IT-system. In the Privacy Impact Assessments various questions on the level of compliance are asked, thereby also increasing the awareness on privacy issues. Besides these impact assessments each IT-system will be documented with regard to the structure and its functioning. This *system documentation* provides inside information on the nature of the data processings and the necessity thereof. In order to assure that personnel is adequately equiped to handle personal data *training* is provided. The issues addressed in the training are the Code of Conduct, the privacy rules, relevant applicable laws and so on.

To complete the compliance structure the data processings, systems and procedures are *audited* on compliance with the Code of Conduct. The audits will take place on a regular basis by the internal audit department. The results of these audits and performance monitoring will be reported in the annual Sustainability Report and therewith form part of the internal accounting scheme.

It is essential to realise that only the 'total package' of measures as explained to you constitutes a minimal standard that convinced the Dutch Data Protection Authority of effective, functioning internal bindingness within the organization.

Another point of interest is that the Dutch Data Protection Authority, in order to be able to advise the minister of justice on the application for a permit under the code of conduct, requires organisations to "show" the Dutch Data Protection Authority two detailed examples of processings. These, together with the elaborate background paper as described in the Working Party document 108, provide the information on which the Dutch Data Protection Authority assess the code in its entirety.

Conclusions

Data protection can only be effective if it manages to keep up to speed with the daily realities of a globalised world. Multinationals, to some extent, need to transfer

data within their organisation, regardless of the national boundaries. The question is if adequate safeguards can also be adduced by non-contractual means. We would say yes, the Binding Corporate Rules offer an opportunity to create a system whereby effective data protection and compliance with the data protection rules go 'hand in hand'. The BCR will ultimately lead to alleviation of administrative burdens and reduce costs for companies and DPAs. So, if flexibility is practised and experience is acquired while handling BCRs and the confidence in this solution grows, both DPAs and multinationals will benefit from the BCRs.

10

International Data Transfers Based on the So-called "Binding Corporate Rules"

Agustín Puente
State Attorney - Head of Legal Department, Spanish Data Protection Agency

Background. The system under Directive 95/46/EC and the "contractual solution"

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, in its Chapter IV regulates international data transfers to third countries not belonging to the European Union.

After starting from the general rule of the requirement of an adequate level of data protection in the destination country (article 25) and an exhaustive listing of a series of circumstances under which transfer will be possible to a state that does not maintain an adequate level of protection (article 26 (1)),[1] the directive in its article 26 (2) provides that "Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country

[1] This must be interpreted as indicated in the "Working document regarding common interpretation of article 26 (1) of Directive 95/46/EC of 24 October 1995", adopted on 25 November 2005 by the article 29 Working Party (WP document 114).

which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses."

The content of this provision resulted in the European Commission and the various data protection authorities, acting through the Working Party created by article 29 of the directive itself (hereinafter the "Article 29 Party"), for years dedicating their efforts to study of the so-called "contractual solution" to enable authorization of international data transfers that could not be authorized based on the existence of an adequate level of protection or on one of the grounds listed in article 26 (1).

The result of the joint work and study undertaken by the European Commission and the supervisory authorities was the adoption of Commission Decisions 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, and 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC.[2]

By means of these decisions the lack of adequate regulation of data protection in the destination state was replaced by the assumption by the data importer, by a contractual instrument binding on it as against the exporter and as against the data subjects, by virtue of a clause in their favour included therein, of the principles and guarantees of the fundamental right of data protection,[3] set forth in Directive 95/46/EC and in the national laws implementing it.

In particular the importer submitted to the legislation of the exporter's state or a set of principles expressly set forth in the Annex to the decisions. In addition, the possibility of onward transfer of the data was limited, in order to prevent the "adequate area" created by the contract from being broken as a result of onward transfer of the data lacking the appropriate guarantees. Finally, the possibility of compensation for any damages to the data subject was guaranteed, by establishment of a clause for joint and several liability in the event of transfers to controllers, or direct liability, in the case of a transfer to processors.

---

[2] In Spain, even prior to adoption of these decisions, Instruction 1/2000 of the Spanish Data Protection Agency of 1 December 2000 in its Fifth Rule already referred to the minimum requirements for contracts for the international transfer of data, with content very similar to that thereafter included in the Commission decisions. It also accepted the validity of such contracts as might be entered into under decisions of the European Union adopted in the future.

[3] Recognized as such by article 8 of the Charter of Fundamental Rights of the European Union.

These decisions were later complemented by Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, proposed by various business associations,[4] amending some of the clauses in the referenced decision.

In the first section of the preamble of this decision a principle is established that is to govern all international data transfers. It states that "in order to facilitate data flows from the Community, it is desirable for data controllers to be able to perform data transfers globally under a single set of data protection rules. In the absence of global data protection standards, standard contractual clauses provide an important tool allowing the transfer of personal data from all Member States under a common set of rules." That is, the creation of alternative models that facilitate international data flows must not prevent the search for common data protection standards that may be commonly applied on a global basis.

Transfers within multinational groups. Need to seek new solutions

The "contractual solution" has proven to be an extremely useful instrument in facilitating international data flows. Nevertheless, this solution has always run up against the problem of transfers within a given corporate group. In that case the contract must be entered into on a joint basis by all of the group companies. Thus, the dynamism of such groups may require constant amendment of the company-specific elements of the contract, depending on the policy for mergers, split-ups or acquisitions undertaken.

In addition, the centralized management of various areas such as human resources within the multinational group, including even the assumption of decision-making regarding such matters by one or more group companies other than the one in which the employee works, is a common and growing reality in multinational groups.[5] This requires adoption of measures facilitating transfer of the

---

[4] International Chamber of Commerce (ICC), Japan Business Council in Europe (JBEC), European Information and Communications Technology Association (EICTA), EU Committee of the American Chamber of Commerce in Belgium (Amcham), Confederation of British Industry (CBI), International Communication Round Table (ICRT) and Federation of European Direct Marketing Associations (FEDMA).

[5] The situation may also be applicable to other activities or policies of the company, such as customer or supplier management, for example.

data needed to make such decisions In addition, availability to all employees on a global basis of, at least, the contact data for their counterparts in other countries is essential to success of the business and the group.

The interchange of these data under certain circumstances may be based on application of the principles established in article 26 (1) of the directive.[6] Nevertheless, a governing instrument is advisable, to guarantee the possibility of these information flows and, at the same time, contribute to generation within the group of what has come to be called "the data protection culture."

The fact that article 26 (2) of the directive refers, in particular, to the possibility that international data transfers will be based on the establishment of certain contractual clauses does not prevent the authorization of international transfers based on instruments other than the contract. The Article 29 Party had already acknowledged this possibility in one of its first documents, related to "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive," approved by the Working Party on 24 July 1998, which devoted its Chapter III to "applying the approach to industry self-regulation,"[7] reaching the following conclusions:

— Self-regulation should be evaluated using the objective and functional approach set out in Chapter One.
— For a self-regulatory instrument to be considered as a valid ingredient of "adequate protection" it must be binding on all the members to whom personal data are transferred and provide for adequate safeguards if data are passed on to non-members.
— The instrument must be transparent and include the basic content of all core data protection principles.
— The instrument must have mechanisms which effectively ensure a good level of general compliance. A system of dissuasive and punitive sanctions is one way of achieving this. Mandatory external audits are another.
— The instrument must provide support and help to individual data subjects

[6] In Spain there have been a number of cases in which it has not been deemed to be necessary to authorize international data transfers under these circumstances, because documentation was provided showing the consent of the data subjects to the transfer, or because such transfers were deemed to be necessary for proper implementation of the contractual relationship between the data subject and the Spanish subsidiary, since certain decisions regarding that relationship had to be taken by the data importer. Nevertheless, currently we must take the interpretation given by already-cited document WP 114 into account.

[7] Although this document refers to sector codes of conduct, it may be considered the basis for current acceptance of the so-called Binding Corporate Rules.

who are faced with a problem involving the processing of their personal data. An easily accessible, impartial and independent body to hear complaints from data subjects and adjudicate on breaches of the code must therefore be in place.

— The instrument must guarantee appropriate redress in cases of non-compliance. A data subject must be able to obtain a remedy for his/her problem and compensation as appropriate."

Taking these precedents into account, it was necessary to investigate the possible existence of a mechanism that could facilitate international data transfers within business groups, without having to use the contract as the required instrument for obtaining authorization therefor.

The solution was reached by adoption by the Article 29 Party on 3 June 2003 of its working document "Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for international data transfers" (WP 74), complemented in 2005 by two new documents, adopted on 14 April of that year by the Working Party, the first of them (WP 107) setting forth a "co-operation procedure for issuing common opinions on adequate safeguards resulting from binding corporate rules," and the second (WP 108) "establishing a model checklist application for approval of binding corporate rules."

Some preliminary questions

Before beginning analysis of the content of these documents, and thus of the "system" applicable to authorization of international transfers based on adoption of binding corporate rules (hereinafter "BCRs"), it is necessary to raise three essential ideas, deriving from those documents and the experience obtained from handling the first cooperation proceedings for authorization of transfers based on the BCRs of a given multinational group, the General Electric group.[8]

The first question is that, by contrast with transfers based on the "contractual solution," in the case of BCRs the analysis procedure should not be just simple

[8] Currently (in July 2006) two other proceedings have commenced, related to the BCRs of Philips (led by the Netherlands data protection authority) and J.P. Morgan Chase (led by the United Kingdom data protection authority). Also, Daimler Chrysler has prepared BCRs (the proceedings would be led by France).

verification that the contract submitted reflects the model incorporated in the Commission decisions that have been cited before.

That is, in our case it is not possible to establish a uniform model to be filled out by the applicant for authorization of international transfers.[9] As stated by WP document 74 of the Article 29 Party, BCRs must be adapted to the reality of the group to which they refer. They cannot be similar to others. Rather the size, business and other circumstances surrounding the transfers referred to therein in each case must be taken into account. The cited document indicates that the BCRs should contain "tailor-made provisions as well as a reasonable level of detail in the description of the data flows, purposes of the processing, etc."

What has just been stated leads to the next relevant question we must now consider. The process for authorization of international data transfers based on BCRs is considered by some to be lengthy and complex, given the need to secure acceptance of the BCRs by the participating authorities. But this process will be simple if the principles governing the fundamental right of data protection have in fact been adopted within the business group applying for the authorization.

In my opinion, this is the most difficult component of BCRs. Mere application for authorization of the transfers based on the BCRs is not sufficient. Rather, for the reasons set forth below, the applicant group in advance must have established mechanisms allowing it to implement the data protection rules set forth in Directive 95/46/EC within the group. Although this task will be simple in companies located in the Member States of the European Union, because the national data protection laws will be applicable to them and must be respected, it also will be necessary that the rules be implemented on a global basis, which implies assumption of a corporate culture that always takes application of data protection principles into account.

Thus, the proceedings for authorization of transfers based on the BCRs will be nothing more than the last step of a complex process that will require true change in the corporate culture of the group on a global basis. In that case, processing the file will be the least complex step in the process.

The last matter that must be noted here is the fact that the authorization proceedings for transfers based on BCRs will require common effort and a mutual

---

[9] This is independent of the fact that the data protection authorities have adopted a document containing a "checklist" that applicants may compare to their actual situations in order to expedite the cooperation proceedings (WP 108). In July 2006 the Data Protection Working Party of the International Chamber of Commerce (ICC) prepared a document called "Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data outside the EU", although in general it cannot replace the particular characteristics of each specific case.

relationship of confidence among all involved in the process. This relationship should not be limited to just the relationship that must necessarily be maintained by the authority leading the proceedings, which we will address later, and the group company serving as spokesman. Rather it should extend to the relationships between the principal authority and the other authorities involved, and the relationships among the various group companies, including the parent, and the authorities participating therein.[10]

Only by means of this continuous relationship of cooperation and confidence may the proceedings be flexible and conclude with effective implementation of the international data movements contemplated by adoption of the BCRs.

Having stated all of the foregoing, now we address the essential elements of the BCRs, both as regards the requirement that they be mandatory and their content, and as regards the procedure to secure the corresponding authorizations of transfers based thereon. We also must mention the problems presented by application of this instrument in countries with a Roman civil tradition, in which unilateral declarations of intent are not legally recognized as a source of obligations.

The mandatory nature and content of BCRs

The purpose of a group's adoption of BCRs is to create, within the group, an "area offering an adequate level of data protection." Thus, BCRs must be analyzed on terms similar to those required for the study of the adequate level of data protection in a given state.

In order for it to be possible to hold that a given state offers an adequate level of data protection, from a substantive point of view it is necessary that its legislation satisfy the data protection principles set forth in the various international instruments adopted in this regard. From a formal point of view, it is necessary that those principles can be guaranteed through an authority that supervises compliance and, in the event of violation or damage to the data subject, adopts the measures necessary to prevent continued violation or damage.

The extrapolation of these requirements into the framework of BCRs implies the necessity, from the point of view of content, to reflect the essential principles

[10] In this regard, the role of the subgroup created within the Article 29 Party has proven to be very interesting regarding the processing of the file related to the General Electric BCRs. This is because it was a pilot experience for implementation of the mechanisms necessary for studying it. Also, from the point of the of the Spanish Data Protection Agency the many contacts maintained with the Spanish subsidiaries of the group and with the highest level data protection officers on a global basis have proven to be extremely useful.

of data protection in an instrument applicable within the group. Regarding application, there must be bodies within its structure that guarantee effective compliance with these principles in the actions of the group companies, and guarantees that it will be able to adopt measures for sanctions or redress in the event of violation or damage to the data subject.

Leaving the content of the BCRs for later, now we must analyze the manner of compliance therewith, which translates into the both internal and external mandatory nature of the rules, which we now address.

Mandatory nature, internal and external

As the name itself indicates, BCRs must be mandatory and binding on all group companies. This binding and mandatory nature must be shown both in the daily operations of the group companies and in their relationships with third parties.

In addition, as may be derived from the various documents of the Article 29 Party to which we have referred before, demonstration of the mandatory nature of the BCRs is essential in order for the authorization for international data transfers based thereon to be effectively obtained.

As has been noted, the mandatory and binding nature of the BCRs must be shown both from an internal point of view and from the perspective of the relationships of the group companies with others, in particular with the data subjects whose data are being processed and onward transferred within the group.

Regarding the internal mandatory nature of the BCRs, the Article 29 Working Party document of 3 June 2003 establishes as a principle that the mandatory nature of the rules must imply that, in practice, both the members of the corporate group and personnel working therein must feel obligated to comply with the internal rules. In this regard, matters that may be relevant include the establishment of sanctions in the case of violation of the rules, the information given to employees and the creation of specific training programs for employees, subcontractors, etc. All of these elements may be indicators of how the individuals within the group actually feel obligated to comply with the rules. In any event, the group must be aware that it will be essential to prove the existence of these mechanisms guaranteeing compliance with the BCRs in order for it to be possible to obtain authorization of the transfers.

The "checklist" contained in WP document 108 contemplates certain matters that must be shown in order to guarantee the effective existence of this internal mandatory nature of BCRs. Thus, it indicates as follows:

— You must ensure compliance with the binding corporate rules by other members of the group. This is particularly important where there is no 'head office' or where the head office is outside the EEA. How this is achieved will depend upon the structure of your organisation but will also be subject to the national laws of the Member States in which your organisation is located (section 5.5).
— Employees must be bound by the rules. This might be achieved by way of specific obligations contained in a contract of employment and by linking observance of the rules with disciplinary procedures for example. In addition, there should be adequate training programmes and senior staff commitment, and the title of the person ultimately responsible within the organisation for compliance should be included in your application (section 5.9).
— You need to show how your binding corporate rules are made binding on subcontractors. Please provide evidence of the type of contractual clauses that you impose on subcontractors and explain how those contracts deal with the consequences of non-compliance (section 5.11).

As may be seen the essential way of demonstrating the existence of this element centres on the existence of training and supervision programs, adopting dissuasive measures that prevent violation of the rules. This would be the case in the event of a processor's incorporation into employment or services agreements of sanctioning measures in the event of violation of data protection principles, which could include even, respectively, termination of the employment relationship or termination of the services agreement.

At the same time the BCRs must bind the corporate group as to its relationships with third parties, in particular the data subjects whose data are processed and transferred to other group companies. This is precisely the element that is essential in order for a transfer based on the BCRs to be held to be adequate.

Thus, in the same way that in the countries where there is an adequate level of data protection the data subject can apply to a supervisory authority to enforce his rights and, if applicable, request adequate redress of the damages caused by unlawful use of his data, it is necessary that the data subject can, in this case, exercise similar mechanisms implying guarantee of his rights and their indemnification if he is damaged.

The various decisions of the Commission related to transfers based on the provision of contractual clauses establish this principal on two basic pillars: the inclusion in the agreement of a clause in favour of the data subject pursuant to which he can enforce the agreement before the data protection authorities and before

the courts, in all respects related to protection of his personal data, and the guarantee of liability of the data exporter in the event of violation of the agreement by the data importer, by means of the rule of joint and several liability or *culpa in eligendo* or *in vigilando,* in such manner that the data subject need not resort to the data importer's jurisdiction to enforce his right.

The guarantee of the external mandatory nature of BCRs must rest on these pillars, as is stated by WP document 74, which addresses this question in its Chapter 3.3.2, indicating that data subjects whose data are within the scope of application of the binding corporate rules must be considered to be "third party beneficiaries" both as regards the unilateral commitments adopted (when national law so permits) and the contractual provisions that exist among the members of the group to establish the binding corporate rules. In this manner, data subjects, as beneficiaries, must be able to enforce compliance with the rules, presenting their claims both to the data protection authorities and to the competent courts.

At the same time it is noted that the scope of the rights of the data subjects must, as a minimum, be comparable to that guaranteed by Commission Decision 2001/947/EC."

Finally, section 5.2.2 of the document indicates that the group applying for authorization must demonstrate that its European union headquarters or the subsidiary to which it has delegated responsibility for data protection has sufficient assets in the Community to cover payment of the amounts owing by reason of violation of the BCRs, or that it has adopted measures to guarantee that it can satisfy such claims.

As is the case regarding the internal mandatory element, WP document 108 establishes certain guidelines in the "checklist" to guarantee satisfaction of this second requirement in the BCRs. Thus, it indicates as follows:

— Individuals covered by the scope of the binding corporate rules must be able to enforce compliance with the rules both via the data protection authorities and the courts (section 5.13).
— Individuals must be able commence claims within the jurisdiction of the member of the group at the origin of the transfer or the EU headquarters or the European member of the group with delegated data protection responsibilities (section 5.14).
— Your application should contain confirmation that the European headquarters of the organisation, or that part of the organisation with delegated data protection responsibilities in the EU, has sufficient assets or has

made appropriate arrangements to enable payment of compensation for any damages resulting from the breach, by any part of the organisation, of the binding corporate rules (section 5.17).

— Your application will need to make clear that the burden of proof with regard to an alleged breach of the rules will rest with the member of the group at the origin of the transfer or the European headquarters or that part of the organisation with delegated data protection responsibilities, regardless of where the claim originates (section 5.19).

— Your application should also include confirmation that you will co-operate with the data protection authorities with regard to any decisions made by the supervisory authority and abide by the advice of the data protection authority with regard to interpretation of WP 74 (section 5.21).

Content of the BCRs

Together with the requirement of the mandatory nature of the BCRs, it is obviously necessary that the rules establish data protection standards allowing the data protection level within the corporate group to be considered to be adequate for the purposes contemplated in Directive 95/46/EC. Thus, from the substantive point of view, it will be necessary for there to be a self-regulation instrument within the company containing the data protection principles contemplated in the community rules and the rules of the Member States, and that they be applied to the specific data flows subject to the rules.

On this point WP document 74 is unequivocal. It indicates that "Compliance with national law is of course a condition sine qua non for any authorisation to be granted."[11]

In particular, the indicated document states that the BCRs must contain the data protection principles referred to in WP document 12, which derive from those already established in the data protection directives approved by the OECD in 1980. These principles are also set forth in the Annex to Decision 2001/497/EC, considered to be the core principles of the data protection right, as follows:

1. Purpose limitation: data must be processed and subsequently used or further communicated only for the specific purposes in Appendix I to the

[11] In fact, in the cases analyzed to date the BCRs include a clause by virtue of which they will be applicable to the extent that the national law of the state where the group company is found does not impose greater obligations, in which case that law is applicable.

Clauses. Data must not be kept longer than necessary for the purposes for which they are transferred.

2. Data quality and proportionality: data must be accurate and, where necessary, kept up to date. The data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: data subjects must be provided with information as to the purposes of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fair processing, unless such information has already been given by the data exporter.
4. Security and confidentiality: technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as unauthorised access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the controller.
5. Rights of access, rectification, erasure and blocking of data: as provided for in Article 12 of Directive 95/46/EC, the data subject must have a right of access to all data relating to him that are processed and, as appropriate, the right to the rectification, erasure or blocking of data the processing of which does not comply with the principles set out in this Appendix, in particular because the data are incomplete or inaccurate. He should also be able to object to the processing of the data relating to him on compelling legitimate grounds relating to his particular situation.
6. Restrictions on onwards transfers: further transfers of personal data from the data importer to another controller established in a third country not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46/EC (onward transfer) may take place only if either:

   (a) data subjects have, in the case of special categories of data, given their unambiguous consent to the onward transfer or, in other cases, have been given the opportunity to object. The minimum information to be provided to data subjects must contain in a language understandable to them:

   — the purposes of the onward transfer,
   — the identification of the data exporter established in the Community,

— the categories of further recipients of the data and the countries of destination, and
— an explanation that, after the onward transfer, the data may be processed by a controller established in a country where there is not an adequate level of protection of the privacy of individuals; or

(b) the data exporter and the data importer agree to the adherence to the Clauses of another controller which thereby becomes a party to the Clauses and assumes the same obligations as the data importer.

7. Special categories of data: where data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union memberships and data concerning health or sex life and data relating to offences, criminal convictions or security measures are processed, additional safeguards should be in place within the meaning of Directive 95/46/EC, in particular, appropriate security measures such as strong encryption for transmission or such as keeping a record of access to sensitive data.
8. Direct marketing: where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.
9. Automated individual decisions: data subjects are entitled not to be subject to a decision which is based solely on automated processing of data, unless other measures are taken to safeguard the individual's legitimate interests as provided for in Article 15(2) of Directive 95/46/EC. Where the purpose of the transfer is the taking of an automated decision as referred to in Article 15 of Directive 95/46/EC, which produces legal effects concerning the individual or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc., the individual should have the right to know the reasoning for this decision.

Nevertheless, as already indicated above, the BCRs must not be a mere list of principles. Rather they must contain provisions custom-designed for the circumstances occurring in the processing and flows of information that arise within the group applying for authorization of its rules. It is so stated in WP document 74 itself. It indicates that the principles must be specified in the BCRs on a practical and realistic basis, in such manner that they fit the activities under-

taken by the organization in the third countries, and that they must be susceptible of understanding and application by those having data protection responsibilities.

In particular, satisfaction of the content requirements reduces to two fundamental matters: limitation of onward transfers of data from the group companies located outside the European Union to third parties not members of the group, and the requirement that any change in the rules be communicated to the authorities involved.

Regarding limitation of onward transfers, the Article 29 Working Party clarifies in its WP document 74 that "transfers from group companies to companies outside the group located outside of the Community will be possible by subscribing the standard contractual clauses adopted by the Commission."

In this way it is intended to guarantee that the "data protection area" resulting from the BCRs is similar to that of a state that offers an adequate level of protection. Thus, in the same way that, in order for personal data to be transferred from the European Union to a third state not having an adequate level, it is necessary to use the "contractual solution," this "solution" is necessary when the data move outside the corporate group subject to the BCRs.

Procedure for cooperation

One of the most significant elements of BCRs is the need for them to support authorization to engage in international data transfers from any of the companies located within Member States of the European Union. The consequence of a different solution would be that transfers authorized in some Member States would not be authorized in others, which would be contrary to the provisions of the community rule itself.[12]

---

[12] Now we should bring up sections 8 and 9 of the Preamble to Directive 95/46/EC, which state as follows: "(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed; (9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of

For this reason, one of the principal efforts of the Article 29 Working Party has been to find minimum standards for an informal procedure that would allow assuring authorization, if not on a common basis, at least by the greatest possible number of Member States,[13] of transfers based on application of the BCRs of a given multinational group.

As a result of the mandate already contained in WP document 74, WP document 107 establishes the basic rules for the so-called "cooperation procedure for issuance of common opinions regarding adequate safeguards resulting from binding corporate rules."

The procedure consists of three basic phases: selection of the so-called "principal authority"; study of the documentation provided by the group and its modification, if necessary; and thereafter processing of the authorization in accordance with the procedures established by the internal law the Member States, when necessary.

Of these three phases, the first and third are particularly sensitive from the point of view of the functions and jurisdiction of the supervisory authorities: the first to avoid what has come to be called "forum shopping"; the third, because the procedure, although seeking coordination among the data protection authorities, in no case may result in mutual recognition by those authorities of the authorizations granted by the others, because that could be contrary to the jurisdiction given to each of them by its national legislation.

The choice of the principal authority thus becomes one of the essential elements in assuring the transparency of the process. It must be governed by objective criteria that assure transparency and seriousness of the process.

For this reason, both the document related to the proceedings and the document governing the content of the so-called "checklist" (WP document 108) establish criteria for determining the authority that will lead the proceedings. Thus it is provided that *"an applicant corporate group should justify the selection of the lead authority on the basis of relevant criteria such as:*

---

implementation of the directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the directive, and this could have an effect on the movement of data within a Member State as well as within the Community."

[13] The reference is to states and not to data protection authorities because under some national laws the authorization is not within the jurisdiction of the authority but rather, for example, within that of the Ministry of Justice after application or a favourable report from the supervisory authority.

a. the location of the group's European headquarters;
b. the location of the company within the group with delegated data protection responsibilities;[14]
c. the location of the company which is best placed (in terms of management function, administrative burden, etc.) to deal with the application and to enforce the binding corporate rules in the group
d. the place where most decisions in terms of the purposes and the means of the processing are taken; and
e. the Member States within the EU from which most transfers outside the EEA will take place."

In any event, as already stated, none of these criteria can be considered to be unique. Rather the appropriate solution likely will be a combination of all of them, in any event avoiding "forum shopping"[15] and assuring free-flowing dialogue between the group and the "principal authority."

To assure compliance with these criteria, the document contemplates a phase for interchange of opinions among the authorities involved to reach, if possible, consensus among all of them as to which is to lead the proceedings.

The second phase is the most relevant regarding substance, but also the simplest as regards the proceedings. It consists of a phase of prior negotiations between the group and the "principal authority" to prepare a draft document. It contains the BCRs as such and the documentation necessary to guarantee satisfaction of the requirement that the BCRs be mandatory. The documentation then is analyzed in detail by all of the authorities involved. They can require the presentation of additional evidence or, if necessary, clarification or amendment of the BCRs themselves.

In any event, because these are cooperation proceedings, it is clear that any authority may withdraw at any time, if it believes that the guarantees provided by the group or the content of the BCRs will not allow authorization of transfers based thereon in accordance with its national legislation. This situation, although not

---

[14] As provided for in the Article 29 Working document number 74, if the headquarters of the corporate group is not in the EU/EEA, the corporate group should appoint a European member with delegated data protection responsibilities in charge of ensuring that any foreign member of the corporate group adjust their processing activities to the undertakings contained in the corporate group, interfacing with the leading authority where appropriate and paying compensation in case of damages resulting from the violation of the binding corporate rules by any member of the corporate group.

[15] Thus it would make no sense to choose, as the principal authority, the authority in the state where the company, by reason of decentralization, has its largest factory if in that country no decisions are taken that are relevant from the point of view of data protection.

desirable,[16] in any event allows assurance of the lawfulness of the decisions adopted by each data protection authority. In this case, the group company located in the territory of the Member State that does not participate in or withdraws from the proceedings must directly apply for authorization of the transfer to its national supervisory authority, or the agency in each case having jurisdiction to authorize the transfer.

Finally, when consensus of the authorities has been reached regarding the admissibility of the BCRs and the satisfaction of the substantive and formal requirements we have been discussing, it will be necessary for them to be submitted for authorization of each of the supervisory authorities or agencies having jurisdiction for that purpose, when so required by national law.

It is so indicated by WP document 107, when it states that "Such confirmation will be regarded by all the participant authorities and the organisation concerned as an agreement to provide the necessary permit or authorisation at national level (if required). However, additional requirements that may exist in each country such as notification or administrative formalities may also have to be complied with."

For example, in the case of Spain it will be necessary to obtain the authorization of the Director of the Spanish Data Protection Agency, contemplated in article 33 of Organic Personal Data Protection Act 15/1999 of 13 December 1999.

As noted before, mutual recognition of the decisions reached by other supervisory authorities is not possible. For this reason, the authorization, if any, granted by the "principal authority" cannot forgo contribution of the documentation that the national law of each Member State requires. In this regard, in systems in which the authorization decision is appealable to the courts[17] it will be appropriate to provide them with the items necessary to make their decisions, which otherwise could not be issued.

The applicability of the BCRs under Spanish law

All the foregoing having been said, the essential problem presented by BCRs in countries whose civil law is of Roman origin, following the French Napoleonic code, is determining whether a mere unilateral commitment to comply with in-

[16] In practice, the solution reached in the event of disagreement by any authority with the content the BCRs has been inclusion in the documentation of a document indicating that the part considered to be contrary to the national law of that authority will not apply to processing in that country.

[17] This is the case in Spain. Decisions of the Director of the Spanish Data Protection Agency conclude administrative proceedings and are subject to disputed administrative appeals.

ternal rules, adopted directly by the governing bodies of the parent of a group, or by all of its members, but in any event lacking contractual value, that is consisting of mere internal operating rules, can guarantee that in the event of violation thereof or damage caused by non-compliance to data subjects, they can enforce their rights or, if applicable, obtain redress for the damages caused to them.

This problem was resolved, as we have seen, by the decisions of the Commission related to standard contractual clauses for international data transfers, by including a clause in favour of the data subject, together with a clause for joint and several liability of the data importer and data exporter, both being concepts fully accepted by the civil codes of the Member States in which this problem exists.

Nevertheless, by contrast with what happens when the transfer is based on a contract between the transferor and destinee of the data, in the case of BCRs there in principle is no requirement of the existence of a contract among the group companies by which they expressly bind themselves for the benefit of the data subject. For this reason, under such circumstances the provisions of the Civil Code would not apply.

In particular, in the case of Spain, article 1089 of the Civil Code provides that "Obligations arise by law, from contracts and quasi-contracts, and from acts and omissions that are unlawful or affected by any kind of negligence." Thus, strictly speaking, the data subject can only demand performance of obligations arising from one of the sources identified in this rule. Therefore, it will be necessary for the obligation undertaken by the group companies to come from one of the sources just indicated. The BCRs must fit within one of the circumstances identified in the rule.

Thus, since there strictly speaking is not any possible recourse to the administrative or judicial authorities in the event of breach of the unilateral declaration of intent, the right to data protection might not be fully guaranteed.

But as we have been indicating, authorization of international data transfers based on the existence of BCRs is necessary for proper functioning of corporate groups. So if countries like Italy, France, Spain and Portugal do not participate in the process it will be very damaging to the adoption of a solution under these circumstances.

In Spain the question was repeatedly analyzed by the supervisory authority, even requesting opinions from experts in the subject matter. After that analysis it was concluded that the unilateral declaration of intent contained in the BCRs must seek to fall within one of the sources of obligations listed by the Civil Code.

In the case that has already been studied, related to the BCRs of the General Electric group, the decision was to transform the unilateral declaration into a contractual instrument.

First it is necessary to note that these BCRs relate only to processing employee data, with the employment relationship, as provided by article 3 of the Spanish Workers Statute, being governed by the Collective Bargaining Agreement, among other sources.

For this reason, the group committed to include a clause in the Collective Bargaining Agreement stating that "The processing of employee personal data will be governed by GE's Employment Data Protection Standards. Employees may seek protection in the data protection principles, and present complaints or advise the company of problems or breaches in this regard using the procedures contemplated in GE's Employment Data Protection Standards, and in accordance with applicable Spanish legislation on data protection".

Since the Collective Bargaining Agreement is the source of the employment relationship, and it is indicated therein that data processing is subject to the BCRs, the application thereof becomes one of the obligations of the company deriving from the employment agreement with the employees, in such manner that there is a contractual link between the company and its employees, based upon which they may enforce the BCRs before the data protection authority and the courts. Thus, the unilateral declaration becomes a part of all employment contracts. So the obligations of the group derive from a contract and fit one of the sources of obligations set forth in article 1089 of the Civil Code.

Nonetheless, this solution applies if the BCRs relate to employee data processing. In other cases, in which the BCRs relate, for example, to customer data processing[18] this solution is not possible. Although it would be possible to include a contractual commitment in future contracts, that would not be possible with respect to contracts already entered into. Thus, the referenced solution would not serve to guarantee the applicability of the BCRs under Spanish law.

The only possible solution in this case is converting the commitment deriving from the group's unilateral declaration into an obligation imposed by law, so application of that rule can be invoked by data subjects before the courts and data protection authorities.[19]

In this regard the draft regulations implementing the Organic Data Protection Act contain a provision whose purpose is precisely to convert the unilateral declaration of intent into an obligation imposed by law. So it is provided that authoriza-

---

[18] This, for example, is the case for Philips.

[19] A similar solution would be adopted in the reform of the French Data Protection Act of 6 August 2004. Its article 69 provides that authorization of international data transfer may be established by decision of the CNIL (Commission nationale de l'informatique et des libertés) in the event of the provision of adequate guarantees, "in particular based on contractual clauses or internal rules related to processing."

tion may be granted for international data transfers within multinational corporate groups when they have adopted internal standards or rules containing the necessary guarantees of respect for privacy and the fundamental right of data protection of data subjects, and also guaranteeing compliance with the principles and exercise of the rights recognized in Organic Act 15/1999 of 13 December 1999 and in these Regulations. In this case, in order to secure authorization of the Director of the Spanish Data Protection Agency it will be necessary for the standards or rules to be binding on the group companies and enforceable in accordance with the Spanish legal system. In any event the authorization of the Director of the Spanish Data Protection Agency will imply enforceability of the provisions of the internal standards or rules by both the Agency and the data subjects.

Conclusions

After analyzing the various problems related to BCRs, the remaining question is whether their implementation as a mechanism for obtaining authorization of international data transfers within multinational groups is or is not beneficial. In my judgment the answer to this question must be affirmative.

In fact, within the framework of the functioning of the groups themselves there is no doubt that implementation of the BCRs will facilitate flows of data transfers within the group. In addition, and more important, implementation of the BCRs will allow the group to publicize the existence of global data protection standards. This, to an ever-increasing extent, will provide it with added value, because it will be able to disclose the existence of a competitive advantage as against other groups that do not implement clear data protection standards within their organizations.

The implementation of the BCRs will be beneficial to the citizen data subjects. Through their disclosure, they will be able to learn of their rights, enjoying more flexible, speedy and public procedures for their exercise.

Implementation of the BCRs also will be an instrument complementary to the educational activities regarding the fundamental right of data protection carried out by supervisory authorities, consistent with their educational and disclosure actions regarding the so-called "data protection culture."

Based on all the foregoing, it is appropriate to conclude that, from all points of view, and without prejudice to the continuing need to adopt measures assuring the flexibility and the ease of implementation of the BCRs, their existence is beneficial for both data protection authorities and the corporate groups themselves, and, as is essential, for the data subjects.

11

Case Study of Binding Corporate Rules

Bojana Bellamy
Global Data Privacy Compliance Lead, Accenture

Thank you very much for this generous invitation and wonderful opportunity to speak to you, to learn, and discuss these very interesting matters which impact not only our companies, our organizations in public sector, but impact all of us, as citizens, as consumers, employees, or customers of insurance companies and banks. Thanks for the sponsors, obviously, for allowing us to be in such lovely historic surroundings.

What I would like to do is, really, just give you a case study of Binding Corporate Rules (BCR). After we had heard our data privacy regulators from Spain and Netherlands, which have given you an excellent overview of what and how is legally possible, what I would like to do is just explain to you how, in Accenture, we have implemented binding corporate rules and, hopefully, will be looking for approval of these with the Date Privacy Commissioners in Europe.

Just a little bit of background for those of you who do not know Accenture.

We are a global IT consulting, outsourcing and technology company which provides services in 50 countries over the world, with about 140,000 employees. Our services—many of you here are probably our clients one way or another—are, indeed, in the area of IT technology and outsourcing so, not only do we have lots of data of our employees, business contacts, website users, but we also have huge

amounts of data of our clients, which we process on behalf of our clients during the provision of our services. So, data privacy is very important on our agenda of all of our executives and top managers from the top to the bottom.

Accenture Binding Corporate Rules approach.

We have had a global data privacy policy—Accenture Code of Business Ethics, we call it Global Data Privacy Policy—implemented in the company since 2000. This is a set of rules which is set on the EU Directive standard. These are the rules and requirements which we apply when handling personal data within Accenture global organization. The Global Data Privacy Policy applies to all personal data of all individuals in their capacity as employees, job applicants, business contacts, website users, suppliers; whichever way they have contact with Accenture, these rules apply to them. The rules apply to all processing of data in all countries. They are compulsory and mandatory for all Accenture country companies where we operate, so the same rules which are set on the EU level apply in the US, in Australia, Japan and, clearly, in the EU—both in countries which have privacy laws and those countries which do not have data protection rules. These rules are also mandatory for all our employees—part of each employee's employment contract specifically mentions compliance with Global Data Privacy Policy. Every employee signs that during the performance of their duties, they will comply with the policy, and treat all personal data in compliance with these rules and national data privacy laws. For Accenture, this is a mean to provide a uniform and high level of protection across Accenture group of companies, which would enable us to transfer data within the company. These transfers would be transfers between a data controller and another data controller within Accenture's group of companies, but also this would cover transfers within the company between one data controller and one data processor. Both of these transfers happen on daily basis—every time one sends an email, every time an employee looks at somebody's name on our global directory; the data transfers happen in HR, in marketing, in recruitment.

Obviously, the Global Data Privacy Policy is just the tip of the iceberg. The Policy is supported by very comprehensive data privacy documentation, sets of guidelines, templates. Furthermore, the Policy is supported by data privacy compliance function—Global Data Privacy Lead, and also regional data privacy leads in EMEA and Americas. For example, our Americas Data Privacy Lead will be implementing data privacy rules and requirements and ensure that our companies in the region also comply with American and Canadian data privacy requirements, as well as Latin American. Finally, in all countries where we operate, we have a data privacy officer. My colleague from Spain is here in the audience, for

example. His Data Privacy Officer role is a part-time role, and his responsibilities are to ensure that our strategy, the policy, the requirements are implemented in Spain in accordance with the Global Data Privacy Policy and Spanish Data Protection Act. So, it is important that this compliance function exists, both at central and local levels, because without this, we would never be able to implement our Policy and strategy. It would just be a dead piece of paper.

Finally, the binding corporate rules and the Privacy Policy is supported by a comprehensive program of education and training, both when people join Accenture and, on-going. In addition, we look at all opportunities to present to various management meetings on data privacy, even if only briefly and to remind people about the importance of data privacy compliance. For example, every time an HR person logs on Accenture HR system, or a recruitment person logs on Recruitment system, any of the systems has a specific data privacy warning which says what is personal data, which has to be used in compliance with global policy and only for purposes which are strictly related to recruitment, employment, etc. Finally, we have also commenced data privacy audits on global and national level, to ensure that, indeed, we comply with our Data Privacy Policy.

In terms of where we are with the approval of our Binding Corporate Rules, we have implemented this concept internally in 2000. However, it has taken some time to revise all the existing documentation and discuss with data privacy authorities. This is a new idea, it took a little bit of time to convince everybody that this is a good idea—the data privacy authorities are looking into this with great interest. Also, we have been waiting to see the developments within the Article 29 Working Party and their Position Paper on BCR and the Model Checklist. We have revised all the documents again, in light of the Art. 29 Working Party requirements. We have submitted formally to one authority, hoping to take the role of the Lead Authority. I hope that I will have a chance to speak to many of data privacy regulators in the audience here, visit and explain our approach . We operate in twenty countries in the EU, so we would like to achieve approval of our BCR in all these countries.

I would like now to explain to you and show what we have in terms of BCR and how they look like. It is important to know that this is all optional—every company has got its own way of doing things. This is just about Accenture's own approach and how I think it works very well in practice. The work that we have done is an on-going work; you can't just write your documents and think this is done. We keep developing documentation, we keep adding, taking away, finding things more or less useful. It is a data privacy pyramid: on top of the pyramid, we have a Global Data Privacy Policy, and all of you who know data privacy and data

protection will recognize how this looks like. The Policy contains the rules, which are explained in simple language, from the EU Directive; it contains the rights of individuals, as you know it, right of access, rectification, objection; it contains instructions for processing on behalf of data controller, between one company to another; it contains complaint handling procedures, where to look for help, etc. And this is all set on the EU standard. Our Global Data Privacy Policy, obviously, is available on company intra-net to all employees worldwide.

Underneath the Global Policy, we have a set of localized data privacy policies for some countries to allow for small differences that exist between countries. So if in Spain, for example, or the UK there is a specific legal requirement to respond to right of access in 30 or 40 days, we would then make a differentiation for that country; but otherwise, the rules are pretty much similar.

Underneath the global data privacy policy, at the moment, we have three sets of guidelines. Currently, this is really where, I think, most of the requests for help and advice come from—so we thought we need to explain to people how these rules apply in specific contexts of employees data, client contact data and system and application design. The client contact guidelines deals with data privacy requirements with things such as, business to businessmarketing and business development and on holding and using information about business contacts. The It System Design, for example, is a simple ten page check-list of the things one has to think about when setting up a new system, new application, data base, or new project in Accenture which involves processing of personal data.

The level below the guidelines is what we call Templates. And again, I am sure you have got similar things. These are the standard wordings; things that we have found very useful and have used in the past five years. For example, there is the wording to put in employment contracts; the wording on data privacy and protection of data that we would like to put in contracts with our contractors, processors, in the EU and outside, the consent notice wording for job application forms, on HR, our employee and client surveys, notice and consent for use of photos. For example, we do not want our people's photos being passed and stored around company internet; so if that happens for a particular legitimate business purpose and business reason, that is allowed, but only with a full informed consent and the right to take that photo away when a project is finished, for example. Finally, there are templates for marketing opt-ins, opt-outs, notices, use of cookies, privacy statement on our websites.

Then further down the pyramid, we have two set of rules which 1) explain how to handle requests from individuals when they exercise their rights under the Policy and data privacy laws—access, rectification, objection to direct marketing—

who has to do what, in what time frame, who gets involved. and 2) the procedure for handling complaints from individuals. In the unlikely event there is a complaint, the rules provide information and guidance on how to handle it, how we will try to rectify, who gets involved, etc.

Finally, at the bottom of the pyramid, there is data privacy inter-company agreement. I have to add that this is the latest addition to our BCR; we didn't have a data privacy inter-company agreement, because we felt that the way we are set up and the way in which our Global Data Privacy Policy functions internally, do provide binding nature to this Policy. However, it has become clear to me in the past two years that, as you have heard from my esteemed previous speakers, legal systems are different, and there are difficulties in some countries to ensure this binding nature vis-à-vis companies within the group and vis-à-vis the individual. So to deal with this problem, we have drafted an inter-company agreement, which is signed between all Accenture companies, currently about 300 globally. This agreement says that all Accenture companies signatories will comply with data privacy policy 90 when processing personal data within Accenture, and they will give rights to individuals to enforce this agreement against anybody who doesn't comply (third party beneficiary rights). We propose to submit and sigh the agreement in those countries where this is necessary as a proof of binding nature of Global Data Privacy Policy.

I have explained what our BCR look like and what we have. Now, I would like to share with you some of our thinking, experience, lessons learned as we were launching this five years ago and living it in the last five years. In particular, I would like to discuss what the drivers were, what made us think about data privacy and why are we making such an effort.

First of all, there were a number of internal factors which really made it compulsory for us to address data privacy on a systematic, global level. First of all, globalization, and all of us living and working in a global village. All of our business processes and functions are truly global, and hence, our systems which support these functions must be global. Our HR system, our Recruitment system, our Accenture websites, CIO organization, which is our information security organization, marketing organization, all of them operate completely globally. It is a big question nowadays as to who is truly a data controller of marketing data from Spain; maybe not Spain, maybe it is the centralised marketing function in the US. This is the fact of life in global companies today; there isn't such a thing as geographical boundaries, there are functional boundaries that we operate within.

When we looked into all of this some years ago, we adopted a mission statement.

The purpose of our data privacy global compliance program was firstly to achieve level of compliance which is good enough in all of the countries where we operate. This is a prime, most important reason; we have to comply, this is the law.

Secondly, we did have to transfer data across Accenture borders, where that was necessary for business purpose; we needed to find a way to do so. This was the second factor, a second driver—enabling legitimate transfers across Accenture global organisation.

Thirdly, respecting individuals' privacy rights—this is not just a empty statement, words on paper; this is part of our Code of Business Ethics. In the Code we say that we will respect individuals' privacy rights, as well as respect the individual. Data privacy is part of that code of business ethics; and, as well, an on-going compliance culture. There is no doubt that compliance and regulation has become crucial for companies existence these days. Those of us who operate in multinational companies are aware that, after a number of scandals which happened in the US (in terms of improper and non-compliant behaviour and non-compliant behaviour of big corporations), compliance has become a very important thing on the agenda of top executives of global companies This also fits very well with the overall "corporate governance and social responsibility" agenda of global companies. Big companies do influence the way this world operates, they influence the lives of many people; and they have got responsibility to ensure when they operate, they operate in an lawful, ethical and proper way. Data privacy is just part of that way of operating.

There were a number of external drivers for our data privacy compliance program as well. Our business is in consulting and outsourcing; we manipulate huge amounts of data of our clients, in telecom, banking, insurance, government sectors. We need to understand data privacy requirements because of clients and client data as well. This is imperative, it's a part of our business, how to handle personal data responsibly, securely and in compliance with data privacy laws and client instructions. There is no doubt that every executive in Accenture would absolutely treat this as a priority. Also, peer pressure is an important element, GE, Daimler Chrysler, Philips, a number of perhaps, big Spanish corporations; all these companies are doing and trying their best. We can't be behind, we have to do it as well. This peer pressure is good for privacy as well. Finally, lots of things which have happened in the past couple of years, particularly, have showed to us that there is increased expectation and sensitivity to data privacy and data protection issues among the general public, amongst our employees, people who we deal with, our job applicants, our client contacts, citizens as well. I don't need to talk to you about all sorts of the big issues that we're all facing now—the balance

between privacy and security, the occurrence of identity theft and security breaches which happen daily and we all read in the press about them, RF ID and biometrics, new technology, Outsourcing and off-shore outsourcing—; so these are all issues which we are facing, which are making the public expect us, big companies, to deal with this. There is really no option but to do so.

In terms of the choices we had to make—whether binding corporate rules or something else, I would like to share, again, with you some of our thinking here. For those of you who perhaps are thinking about what the best options are, there is no an easy option, it is not easy to ensure compliance, it is not easy to find the best way to transfer data in compliance with the law. But I think binding corporate rules is really the future. Personally, I believe that for those companies who operate across number of borders, it is probably the only viable solution. For those companies who want to do the right thing, it is probably the best solution. It completely suits companies like Accenture, because of our global and integrated nature where, as I've said, we don't operate by geography, we operate by functions. It offers a very practical workable way for treating personal data of people within the company; one legal regime for all data. I sometimes fail to understand how in practice can companies comply and implement with other methods and instruments of international data transfers, such as US Safe Harbour rules. How do companies differentiate in their systems, databases between European data vis-à-vis US data, and how do they apply particular rules to European data and particular rules to US data? I think that is very difficult and may cost another several million to set up a system in a way in which different data is treated differently. One legal regime for all data is what makes sense; it is easy to communicate, it is easy to explain to people, it is easy to learn—and it really works.

In my daily work, I am constantly amazed and pleased to see my colleagues across the world understanding these privacy rules and doing their best to apply them and consult with my team. For example, we have people in the US exercising right of access, because we give them the possibility to do so, even though their law does not provide for this. You can't treat your employees differently; you can't apply something to one and something else to the others. Our experience shows that global rules and requirements does really work—in some instances we have a better level of compliance and adherence to data privacy requirements in some functions in the US that we would have in Europe. Our audits have actually shown this.

Looking at Article 26-1, the derogations in the EU Directive from international data transfers prohibition; they are just derogations, they are exceptions to the rule, which have to be applied restrictively. They don't provide adequate level of

protection, really; they don't provide real, true protection to the individuals; they are just there to allow transfer in a particular case. But our transfers are not particular, they happen all the time, hence using the derogations in Art. 26-1 does not really suit. We don't have time to ask ourselves before we push a button to transfer personal data what particular derogation applies in this case, is it employment contract? Is it necessity? Is it consent? Is it necessity for public interest? It does not really work like that in practice—the reality is much quicker, much faster and we have to ensure that peoples' privacy and data are protected wherever it is held and used. Taking into account the Article 29 Working Party recent paper on how these derogations should be applied, they are to be applied very narrowly—for most situations, they probably wouldn't work in a global context and they really are not sufficient to cover every day uses and transfers of data. For example, the data about business contacts, how do you transfer this for marketing purposes, Business to Business marketing, for a number of uses to the US, where your marketing function is situated? A specific written consent may be difficult to execute in business to business scenario and may not be realistic. Isn't it better to provide the same level of protection in the US for that personal data and use it in accordance with data privacy rules?

BCR approach is privacy enhancing, it is privacy friendly and works in practice. Part of my role is to do privacy impact assessment—every project, every application, every system has to be reviewed and approved by my team. In that context, it is easy to apply one set of rules, and it does get done much better and much more quickly.

Accenture also looked into other options—Safe Harbour, consent, derogations, the EU Standard Contractual Clauses. I don't think that they work for us. For example, the role of consent in employment field is dubious, anyway—is it freely given? Is it specific? Is it easy? What if somebody says no, will you then have system for those who have said no, and system for those who have said yes? Systems and global companies are not set up like that. Furthermore, Safe Harbour just covers the US. What about the rest of the world and other countries where data is transferred or accessed from? It is not a truly global solution.

Finally, let me just say one thought about the EU standard clauses. Whilst I think they were a very useful mechanism, and they still continue to be so for particular transfers one-to-one, I don't think that they really are very applicable, nor easy to apply in the context of multi-national companies, where transfers happen all the time between multi-parties, multi-controllers, multi-processors, multi-transfers. Also, I do not think that the standard clauses really achieve data privacy compliance. They often become just a piece of paper, which gets signed and goes in

the filing cabinet. and nobody does anything about it. Hence, Binding Corporate Rules is a much better way forward for global compliance and international data tranfsers.

In conclusion, Binding Corporate Rules is a serious commitment; this is not for everybody. BCR suits those companies who can find the resources, and conceptually accept this as a way of doing business. BCR is not a project, it's not something that you do, tick a box at the end and forget about you. This is a way of living and behaving on a daily basis within a global company. It isn't just a mechanism for international data transfers. Of course, it allows transfering data where there is a business need and in compliance with the law; but BCR actually create the rules where the rules do not exist ; it creates a uniform and high level of privacy protection within the company which has to be upheld. So, in that sense, it is a serious commitment, because the company has to ensure that once the document is adopted the company complies with it and maintain the level. Of course, drafting and having the regulatory approval is a big and long process, but really, the real work starts afterwards—to ensure that all your companies globally, all your functions, all your people actually understand and comply with these rules. In Accenture, we have proved that this approach of BCR works in practice. Would we do it again? The answer is yes.

12

Adoption of Binding Corporate Rules: Action Plan

Eduardo Ustarán
Partner, Field Fisher Waterhouse LLP, London

Those of us involved in data protection have probably spent years debating international transfers. Thus when the Article 29 Working Party in 2003 for the first time recognized the idea of binding corporate rules as a valid mechanism for legitimizing such transfers, the truth is that heaven opened up for us, for a very simple reason. The use of binding corporate rules is the only realistic way of satisfying legal obligations regarding data processing on an international basis.

Based on my experience over recent years, my presentation concentrates on what we might call the action plan for an organization planning to adopt binding corporate rules.

Justification

Let's not kid ourselves. A project like binding corporate rules is a project of great magnitude. Therefore from the point of view of a company there must be a business justification. From my point of view it is really very simple, because it is a matter of logic. If for an organization respecting privacy is an operating principle and

part of its culture, the logical thing is for it to be established by means of binding corporate rules.

It also is a matter of legal certainty. In a world like that of data protection, where there is no black or white, less than in any other branch of law, there is nothing that gives greater certainty than having the vote of confidence of a data protection authority. It also is a matter of efficiency, since we live in a world that favours consolidation and the adoption of a uniform management system. When uniform overall management is applied to data management is it is a much more efficient way of operating.

Finally, employees of companies and the persons we deal with on a day-to-day basis do not understand the jargon that appears in the various legislative texts. Therefore, the only way to make the legislation and data protection system comprehensible is to involve everyone and become familiar with these kinds of rules, in such manner that an enterprise can state them and share them with its employees.

But ultimately what matters in a company, and I think we would all agree, is results. We all have bosses and all bosses want results. Binding corporate rules are a key factor in reducing risks of violation and therefore risks of sanctions. And not just this. They also are a tool for managing a part of the company's assets (intangible, but real), that being personal data. In fact binding corporate rules contribute in a very significant way to increasing the profitability of companies.

Documentation required

The question then is: "Now what do we do?" In the first place, we must cover the matter of required documentation. Last year the Article 29 Working Party approved a checklist that, when examined carefully, refers to three sets of documents that must be presented. First is the general information regarding the company. The purpose is to contribute, in a logical manner, to choice and justification of the point of entry, the so-called "lead authority." This first set of documents is the one that will help us convince the relevant authority that it is the one that must approve and guide the company during the process of adoption and approval.

There is a second set of documents that probably is the most important, because in fact it is a summary of how the rules will function and how they will be made truly binding. The reason this set of documents is so important is that it demonstrates that the rules in fact will work, which is the purpose and the end sought by the authorities.

Finally there are the documents that set forth the binding corporate rules as such. The question I am often asked is: "Do we have to present everything? Everything we have?" The answer is that it is impossible to present everything, because the documents are to be generated in accordance with the concept of binding corporate rules to be implemented. What is important, then, is presenting documents at all levels, from the summary of how the rules will function, to examples of given policies that will be applied to certain departments, or specific contracts that will be applied to certain relationships, in such manner that the procedures that will be in place are demonstrated.

Project phases

It remains to ask what steps must be taken in order for an organization actually to receive approval of the rules. Binding corporate rules projects normally have three phases. The first is the initial decision phase, during which the company has to make certain decisions that will guide the process. The first decision in fact is whether or not to do it. What one has to consider is whether there is conviction within the organization to adopt a plan for compliance with data protection legislation on an overall basis. Because if there is no such conviction, what is most likely is that such a system cannot work.

Then one has to choose the team and the manner of managing it. Of course there is going to be a leader, a person that will be the visible face within the company and before the public when guiding the organization. And not just a leader, but also a team behind that person. The team must include top executives that support the idea, legal representatives that assist within the company in clarifying concepts, and representatives at the international level, so that within subsidiaries there is the so-called "buy-in," that is the conviction within the company that the system of binding corporate rules will work.

Another fundamental decision is the scope of application. By this I mean to what kinds of data the binding corporate rules will apply. One option is to apply the system to all personal data used within a company. But is this possible? Or is it better to begin with specified data, for example employee data, customer data, or perhaps data we are sure flows on an international basis rather than data that will be processed only on a national basis? This decision is very important when determining the amount of work that will be required.

Another important decision is choosing the "lead authority" from among the data protection authorities that will guide us during the process. In some cases

this may be obvious. But in many other cases it is not easy to determine whether the European data protection lead authority will be in Spain, in the United Kingdom, or in Belgium, for example. This is a strategic decision, not only from the point of view of the one that is to be the point of entry, but also as regards what other authorities will have to participate. Because if a company operates in all Member States of the European Union, does this mean that we will have to adopt the plan in 25 states at the same time? Or are we going to select certain States that for internal reasons are more significant when justifying transfers?

And finally, there is a structural decision. The situation I have found myself in on several occasions is that it is not possible to determine the structure without completing the following step, which is the second phase: internal analysis. This analysis will allow us to decide what work is necessary for approval and adoption of the rules. A first step is collecting information on how the company operates, the flows of personal data and the processes and rules already in effect.

Most companies already have certain processes in place that are applied internally and addressed to compliance with the legislation. It is very important to identify these kinds of documents and procedures, because of course it will be simpler and more efficient to start with what we already have. Then what one has to do is to compare where we are and where we wish to be, to identify the "gap," and prepare a weekly or monthly plan with budgets to see exactly how we are going to approach the project.

A part of this plan is preparing what I would call the map. The map is the document that is going to guide not only us, but also the authorities involved in the process. It is a process that will last for some time. The map is a guide showing us the road. Finally it is possible to draft and implement the rules and procedures we believe are necessary.

The last phase is probably the simplest, but not for that reason the least important. This is the application phase. This phase begins at the same time as the preceding phases, in the sense that it is clearly advisable not to wait for completion of the prior phases for an initial interchange with the authority that is to be the point of entry. The purpose of this initial interchange is to get to know each other in the manner of a small courtship of the company and the authority, to see exactly where the strengths and weaknesses lie. There must be teamwork between the organization and the authorities.

In fact, it is also advisable to present draft applications showing the existing kinds of policies, internal codes and contracts, so the authority can guide the company. In this way it will be much easier to succeed and demonstrate success, externally and internally.

Final recommendations

I conclude with a series of final recommendations summarizing my experience in this area. The first is that one must approach binding corporate rules as an investment. If it is seen as an investment, what it actually gives us is a competitive advantage.

Another point to be emphasized is that it is essential to use what one already has. If we have to invent everything and start from zero it will be a very difficult and very costly process. The good thing is that the authorities are inclined to cooperate more than ever. The authorities are allies of companies in this area, since their interest in the system functioning is the same, if not greater.

Finally I would stress that in order for a binding corporate rules project to succeed it is necessary to have a great deal of imagination and a great deal of will.

13

The Point of View on BCRs from a Large International Business Organization

Christopher Kuner
Chairman of The International Chamber of Commerce

ICC has member organizations and companies in over 130 countries, and is almost 90 years old. People may know us for institutions like the ICC Court of Arbitration, the Uniform Customs and Practices for Documentary Credits, but we also have a long-standing taskforce on data protection, of which I'm honoured to be the Chairman.

Binding corporate rules are real world data protection. This is because some of the other legal bases in the directive for transferring personal data outside the EU often do not work very well in practice. Some of them are limited to a specific country, such as adequacy decisions, or the US Safe Harbour system. Others are too restricted, such as use of the exceptions in Article 26. Consent, for example, often just does not work very well in practice. Or they are too cumbersome, so that having hundreds of affiliates around the world signing standard contractual clauses is very, very cumbersome and lengthy and does not work very well.

One point which is very important to make is a question that we have to ask at the beginning: why do we have BCRs? Is this just a way to reduce the burden on large multi-national companies? The answer is no. If the only reason for BCRs was to save money for multi-national companies, this would not be an adequate justification for their existence. It is important to say that BCRs have benefits not only

for companies, but also for individuals, and for data protection authorities. For individuals, because they provide a higher level of data protection, and also provide more transparency. It is difficult for individuals to find out information about model contracts that have been signed, for example. It is much more transparent if there is a set of BCRs which they can have access to. It also provides benefits for data protection authorities; they don't have to have thousands of contracts filed with them all the time. It is a much more efficient way to provide adequate protection. And it is also important to note that this is a very interesting way to raise the level of data protection throughout the world. When a company with an affiliate in Saudi Arabia for example, has binding corporate rules and implements them there, it means there will be a little island of adequacy in that country. As these BCRs are implemented in companies throughout the world, this will gradually spread the ideas of the directive in other countries. So, this is another way to gradually increase, maybe, the level of data protection around the world.

As BCRs have become more and more recognized over the last few years, there have been a few milestones along the road. There was a hearing of the Article 29 Working Party in the Hague in 2004. Since then, the Working Party 29 has issued two papers on BCRs. We now have had the first approvals in various countries including, perhaps soon, even in Spain. So they are really spreading around the Community.

The ICC issued a report on BCRs in October of 2004. This report is available on the internet. This report contains a survey from different legal systems around the world and around the Community about the legally binding nature of BCRs, and it also indicates the thinking of companies and lawyers going beyond data protection law, because it is also important to remember that these sorts of company codes have been used for decades in other areas. This is not something that's new to companies; there are codes of practice on money laundering, on various ethical issues, on all sorts of areas. So this is just an extension to data protection of something that has already existed, and it also shows that there are different ways to achieve the legally binding nature of BCRs, depending on the legal system.

Much discussion has been had about the enforceability of BCRs. This is obviously something very important. If BCRs are to be accepted, it is important that they be seen as legally binding. They are not just a recommendation or a guideline, but something that can be enforced if there is a dispute or a problem. Our report shows that this binding nature can be obtained through a variety of practical mechanisms. First of all, through the internal structure of the company, and the fact that there are lines of authority and possibilities for management to direct

different entities to act in a certain way. Also, through employment contracts, where employees have to sign a contract that they will all comply with the BCRs, and the fact that these can be enforced by disciplinary sanctions. Any company with BCRs will also have to have a system of internal compliance officers whose job is to enforce the BCRs. Many companies are also subject to compliance with other laws; the financial services sector and the pharmaceutical sector are examples. This will often include an obligation to implement codes in certain areas. Data protection compliance can be seen as a sort of ethical issue or a corporate governance issue. So, to the extent that companies are subject to corporate governance obligations, they will also be subject to obligations in the data protection area. There are also the more sort of classical, legal ways of enforcement, which work in some jurisdictions better than in other, such as having third-party beneficiary rights. The result is that there are many different ways to achieve this binding nature, and this can often be achieved through a combination of mechanisms.

Now, in addition to looking at the nature of BCRs: what they are, and how they are implemented, I thought it would be interesting to also look a bit at some of the challenges and, problems that currently exist with regard to BCRs. We have made a lot of progress but we still have a long way to go before they are really fully accepted. What are some of the issues, in practice? The negotiations often are too slow. This can be the fault of either side. It can be a fault of the data protection authority or of the company. But it is still necessary to go around and have extensive conversations with various regulators, and this can take quite a long time. There needs to be a lot more harmonization. Maybe it is not necessary to have a model BCR, because companies have different structures, and there can not just be one model for this. But we could make much more use, for example, of templates, and different model documents. So that when a company wants to do BCRs, they do not have to start from zero because there are documents they can orient themselves around in practice. We need to do this more. ICC will soon propose to the Working Party a standard application form for BCRs which is designed to be used for applications for the approval of BCRs in all Member States.

This cooperation procedure of the Working Party, which maybe making slow progress, is not working as well as it should. And I really think that we need to have the European Commission consider further action; because if BCRs are a way to transfer data borders in a globalized world, this should really be something that needs to be dealt with at a European level and not just nationally.

We really need a Pan-European approval process for BCRs. This coordinated procedure is maybe going to develop in the future, but it is still a bit slow. If we

look in other areas of Community law, there are many areas where it is not necessary to have approval from each Member State; for example, the approval of pharmaceutical drugs doesn't require negotiating or getting the approval of each single Member State regulatory authority. So we do not see the substantive reason to have approval of each data protection authority. It should also be possible to have adequacy decisions or some sort of centralized decision approving BCRs. At the moment, companies are caught a bit in the middle, because many companies want to use BCRs, but they realize if they go down this road, they are going to be starting a very lengthy, very expensive and complicated procedure.

We have had a lot of talk today, also, about large multi-national companies using BCRs. BCRs can be a huge advantage and utility for small and medium-size companies. Particularly a medium-size company that does not have the resources to sign all sorts of model clauses and simply wants to implement a solution for data transfers which they can use continually in the future. So, in a way, this is something that could also serve the needs of small and medium companies. But at the moment, they are a bit scared off because they see that this is something only the biggest companies are doing. And they are worried about opening a Pandora's box that is going to continue for several years.

Europe is not the only region of the world which is working on BCRs. There is a group in the Asia-Pacific region called APEC, which is the Asia-Pacific Economic Cooperation Group. It includes all of the economies of the Asia-Pacific region, including the US, Mexico, and Australia, etc. They are now, having already approved privacy principles, beginning discussions on BCRs. This was discussed, at their last meeting in March in Vietnam, and they are planning to have further workshops on BCRs throughout this year. We still see BCRs too much as a sort of EU and US issue. In other words, large US companies trying to get approval in the EU. Actually, this subject is much broader. Companies are not only transferring data from Europe to the US, they are transferring it around the world. We have to be a bit humble when we realize between the EU and the US, we have about 700 million people. Well, in Asia, depending on how you count it, we have either 2.1 billion people or, including India and Pakistan, we have over 3 billion people. So Asia is between 3 and 5 times larger than we are. If Asia begins implementing BCRs and using them, the risk is that they will already have something in place while we will be engaged in all sorts of arcane legal discussions about how to make them legally binding. So, if we do not want to be overtaken, we need to have quicker progress in this area.

14

Practical Experience on Binding Corporate Rules

John Vasallo
Chief Privacy Leader
Senior Counsel of General Electric

I have much experience on data privacy because we have been working on it a long time. The notion of having to deal with a thousand different small pieces of law, thus, and trying to combine it into a unitary approach, I think has been a philosophical and a practical reason for Binding Corporate Rules (BCRs) coming into existence. The openness with which the dialogue amongst the data protection agencies and companies like ours, and Philips, and Daimler-Chrysler [is encouraging] because we have been competitors and colleagues working together on this issue, together with all of you. I have already spoken to the DPAs on two past occasions, and I feel very flattered that we have come such a long way, and that so many references were made to us. In effect, we are in a way creating law together, creating a concept together. It is humiliating and humbling, knowing that you have to break new ground, but there are issues and there are challenges ahead.

Here, I will continue the dialogue and explain to you the philosophy of the internal processes and the protection that GE, in its culture, and systems, applies to its employees is and how it works. I hope that when we discuss this together, we can continue after this. Because this is not the end today, we must continue towards what Billy Hawkes called yesterday the 'Nirvana' of a global privacy protection

legal system. In fact, the title of my presentation reflects the fact that we think it is a global privacy network, a framework. But it is only one step in the process. We are not yet there. We like to take challenges at GE, and I think that once we have finished with the BCRs for employees, we will explore the notion of BCR for customers and suppliers and other third parties, and find a way to deal with that as well.

We would like to engage with you on the larger global harmonization which many of yesterday's sessions dealt with. You will see what General Electric does. We are in very many segments, very many businesses, and within our six structures of businesses, there are a number of other sub-businesses. The title for this section is "Data Protection and Economic Activity." But that title could equally deal with many other subjects, and not with only BCRs. In fact, Professor Rodotá's speech yesterday gave me a lot of ideas about how many of the GE's segments and businesses interact, and are involved in that area of innovation that were discussed yesterday; for example the new solutions to RFIDs, sensors, and nano-technical diagnostic imaging. We are also involved in consumer finance, so we have a lot of data of private individuals. And we have equipment leasing of cars, airplanes, containers. We would like to know with the GPS systems where our property is; but, of course, that also intrudes into [the privacy of] the user of that property.

So all these areas could have been the subjects, equally, of this presentation, rather than the internal workings of BCR because if we can get to that utopia of a common global system, and if you can, as DPAs, spend more of your time discussing the future data privacy areas, the future worlds where intrusion will happen, the future protection for our citizens, and set standards together in advance or together with technological research; then companies and citizens are going to be doubly protected. First, because we know what the standards are going to be; and second, because we will be able to assign our resources to do the research and development that is necessary to produce the right products that fit with the standards that the authorities are being asked to create for the citizens. Where these standards set, we in the industry would be able to discover and bring to the market adequate technologies, rather than the other way around, with the technologies coming first, and the law constantly chasing. That is a bit too far away, but by putting these systems that reduce the burden on DPAs in place—and BCR is one of them—we will liberate the data protection agencies to be able to spend more of their time in that creative mode of setting standards.

Let me explain why GE moved into this sort of leadership role of finding the solution. We have about 150 billion dollars of sales and over 315 thousand employees, half of which are outside the United States. The European Union is a

very big part of our business and has a huge number of our employees. We are present in all of the Member States. With such a growing international base, we have one thing that makes us function, and that is our common culture. We have an internal culture which I will try to define to you that is common to all our activities. The big difference is our culture of integrity. This was not just created for data privacy issues. It is a culture of compliance and commitment to compliance, an internal support and control system that gives both rights and sanctions to all employees and stakeholders in the company. We apply our rules not just to our own employees, but also to subsidiaries, joint ventures, suppliers, and to customers when we can. Suppliers are easier, customers are more difficult because you cannot impose on them. But you can apply the same rules to their information. And we do this through a process of internal communications.

The foundation of all of our values is integrity. It is, for us, a business concept. It makes business sense to have a culture of compliance. It makes business sense to create trust with your customers, with your suppliers, with your employees, with future employees, with young students looking for work, with labourers who want to improve their standards of living, with suppliers and their staff in far-away countries that lack the same level of the rule of law. But we bring integrity in all of these areas because we have this common set of rules that will apply around the world.

How do we impart this information about our internal culture? We have different layers of rules. For all new employees and also for existing employees, we have contained all our policies in a document called "The Spirit and Letter." Everybody has to acknowledge receipt of it, and there is on-line training attached to all the different principles and rules that this book contains. It contains obligations on the company, but also on the employees of the company. It applies not only to employees, but also to all subsidiaries, what we call control affiliates, throughout the world. Amongst these policies and within that set of rules, we find the protection of the employees both when it comes to their privacy rights, and also their employment rights. In fact, we can say that we have a hierarchy of policies.

As mentioned before, there is a need to have layers, to have different levels of structures with varying sanctions; and this is how we have set out our "Spirit and Letter." It is the principle, the highest level of policy, and within that we have a number of policies. For data privacy, we have a specific set of rules. This is the employment data protection standards which we now also call externally the BCRs. As we proceed down into the actual details of the "Spirit and Letter," you will see that we do have a generic privacy policy, it includes policies governing the use of the collection of the data, the protection of its use when it is being held, and the

implementation of the responsible procedures and compliance. In fact, Mr. Jacob Konstamm made three positive points that are necessary to have consistent application. The first was implementation; the second was documentation; and the third was ensuring company compliance. This is fundamental already in our basic principles of the privacy policy and it defines the personal data, not just the data of employees and not just consumers, but broadly includes all data of anybody who comes into contact with the company.

Let us begin by looking a bit at how we communicate our standards to the employees. We have a very simple website called integrity the employees use. It is available in 26 different languages. Through a simple click you can get to all the links to advice, information, the law, the existing practice, and to hot links. Should an employee have any need to ask questions, or feels that there is a breach occurring, they can go into the "Raise a Concern" page, which will help them bring their concern to the attention of the company. They can also see that their concern will be followed through. There are 13 policies, and they are written in a user-friendly language, because providing just a link to the law is not sufficient in many cases. Often companies need to distill the law down into practical, step-by-step explanations. Linked to each of these policies, including the privacy policy and the data protection standards, we have training on-line. Employees are obliged and reminded by the system to complete web-based training every 18 months. Direct managers or superiors have the ability to see that their staff have completed the training. And because it is integrated into our network; it will appear as a reminder through the employees' daily computer use.

Our structure, internally, is built upon very complete top to bottom and bottom to top processes and systems which insure that they have the attention of the highest levels of the company. In fact, they go all the way up to the Board. We have a reporting structure to a Policy Compliance Review Board, which reviews regularly all the 13 policies. We also have a company corporate Chief Privacy Leader. Furthermore, similar to Accenture and other companies, we have a Privacy Leader for every region. We call them PLs in GE. There are Privacy Leaders in every business and in every country. Within the businesses, there is also an Internal Review Board, which looks at all the complaints and at all the results of the audits, and does a summary that it reports up to the Policy Compliance Review Board which conducts business reviews. The report goes through, for example, aircraft engines, or it goes through energy, or it goes through the media companies of GE, because they are specialized. It examines the global world, country by country, their main issues, how many cases have we had and how many disciplinary

actions have been taken. These issues are reported to the board, which then summarizes it and reports it to the Corporate Board of GE.

We also do it for every country. So we have a cross-business reporting structure that collects the same complaints, actions, and sanctions that have been taken on all the 13 policies, including the privacy policies; but it crosses across different businesses. Because we have, of course, different sectors, which have different types of employees and different types of activities. We can have an intellectual activity if we are selling financial services, or a physical activity if we are producing light bulbs.

And of course, there is different needs for the data, we collect data about our employees and data about our customers in different ways. But we cross by country because there are cultural differences in different countries. We may get a country which is very litigious, where we have a lot of people, or a very small country where people know each other where we get a lot of complaints about unfair use of data; or we can get a very huge country which is less litigious, which is much more computerized, much more modern and, therefore, we find different types of issues in that country. So we tackle it both from the each business sector and across each country.

These reports are done regularly every year, and we have statistics about them. The Board of Directors is involved regularly. It has regular updates through its audit committee of all the reports that go to the Review Board, We do our Review Board locally with all our businesses, and that report goes into the system. However, to collect the data, we have a Chief Compliance Officer in charge of all the 13 issues. Then we have the internal audit. We have 400 auditors world-wide, 100 in Europe, and they constantly go around all the sites—from the furthest away sites with two or three employees to the largest sites with 2000 employees—and do audits, both financial and compliance. They do this regularly, two to three times a year.

We also do dawn raids. We do dawn raids internally on our own companies. We take staff from my office or from different offices, not the compliance leaders but lawyers from different parts of the business, and knock on the door in the morning and say. "I am the competition authority. I've come to check on your retention of data." Then we watch to see what happens and how the company reacts to that. Is the staff prepared for it? Where is the data? Do they have a person in charge? Etcetera, etcetera. We report on all of this information.

Finally, we have the global ombudsmen network, in which we have 117 ombudspersons in Europe alone. They are within the businesses, and they are often known to the people on the floor. There are also ombudsmen for the country that

are less well-known to the people, if one wants to go and discuss a complaint. And then we have ombudsmen in the headquarters in Brussels, in the headquarters in London, and in the headquarters in Fairfield. So this is a double hierarchy. We have the hierarchy of the rules and the hierarchy of the controls and training.

More important are the actual protections that the employees have. They have the protection of all these controls, of the opportunity to go to make complaints, to have their concerns heard, of knowing that compliance is being monitored at the very top of the company, from the very top to the Board. They also have some additional opportunities, additional protections that are in the contract with all new employees. The new employees enter into their employment contract by committing not to publish or disclose or use any of the data of others in the company. So that is an extra, additional help; control for third-party and other employees.

Additionally, everybody is obliged to report violations, according to the "Spirit and Letter" that they acknowledged when we joined the company, so they feel that they should also report any breaches they know of. It is an obligation upon every one of us to report breaches and, therefore, protect those other employees who might have a breach occurring against them. Retaliation against anybody who reports a breach is prohibited by the company rules, and there are also sanctions against the company if it does not abide by that policy. We can be taken to court and have to pay penalties.

We also have audits by third parties. We will also go to anybody who enters into a contract with GE, send our auditors to them, and insure that they also commit to protect data, consistent with our own BCRs. This includes their data vis-à-vis their own employees, so they are third parties to us. We have had cases where we have terminated contracts, agreements, with third-party representatives who have not abided by this principle because we follow this very seriously.

Now, transparency was also a very important part of the conditions that were mentioned for data privacy protection rules to be acceptable to the authorities. Not only must our internal process function. They must also be seen to function. So the employees themselves are actually the guardians, more or less, of their own data. When employees enter the electronic systems of GE, as they will use the Internet and the website, they get consistent references to the existing rules; they get reference to the documents that are available. They are constantly reminded, as they use the data, that they have to follow the rules, and what the rules are. They can also get access to the rights of access, rectification, and objection that has been consistently visibly employed on all work pages where their data may or may not have been used. They are given a link to be able to go in and to make any

necessary corrections. They have, on the other hand, a direct line open consistently to people they know—their HR manager, their direct superior—who have, as we mentioned earlier, an obligation to report any violations. They have opportunities to go to the ombudsmen, who may or may not be, according to their personal wishes, a person they know or a person at another site. And all this data about who is who and what numbers are available come at an easy click, and is very visibly noted upon the website.

We maintain a record of this data. For example, last year, we had about 755 reports to the ombudsmen system in Europe, and many of these contacts are simple information requests, but about 30% of them were be for compliance, for breaches of one of the 13 policies of GE. The major countries where the system is used in Europe are Hungary and the United Kingdom. This is not surprising because we have the largest number of employees in those two countries. Germany and France come a close second following the UK and Hungary. Many other countries, Netherlands for example, do not as many contacts. In still other countries like Italy, Spain, and Greece, we've had less than 10 complaints or contacts to the ombudsmen system in a year. These are not very large numbers. There are all the normal contacts that have happened to the management system—when an employee speaks to his or her superior and would like to bring a complaint.

Finally, the most important area, is that any business leader in GE, is responsible to make sure that they have a business Privacy Leader installed in his or her business however small the business unit is. We have given the legal right to all our employees to bring claims to their local DPA; and we have committed in our BCRs to respond diligently to the DPAs. In fact, the cooperation with the DPAs has been extremely close. This has been especially true in these last two years, as we have been not only discussing the concepts and the theories relating to the BCRs, but the actual practical issues country by country. We are willing to amend our EU addendum that would allow EU employees of GE to bring the claims in the country where they work, even when the breach has taken place in another country. This would bring the local requirement of the courts and the authorities in the country where they feel most comfortable. We also have the right to use the local entity to support. We will continue to provide this information to all our employees, and to insure that the enforcement takes place.

Finally, there are some conclusions regarding why we think BCR's are effective: they are user friendly, they are visible; they bind both the GE companies and the employees, so it's a common binding. They are harmonized, they apply right across the world; and they are consistent with our compliance policy, our integrity culture that is the basis for all our doing business. BCRs are more positive than

the other solutions. In contrast, Safe Harbour agreements and contractual clauses are too complex, too difficult to understand, too difficult to see.

How many approvals do we have? We have close to around twelve that have been approved; seven are clearly approved; two, Spain and Sweden are approved, but require some further filings. Hungary cannot approve it by their law, but have approved it in spirit. So, we have come a long way. We have had a very good cooperation with the authorities; and we hope that we can terminate this process within the next few months, that we can move on to discuss other areas of similar processes, the concept of binding internal rules to other areas of data privacy.

Part iv

DATA PROTECTION AND THE FIGHT AGAINST FRAUD

15

New European Proposals for Combating Fraud in the Financial Sector: The Experience of the Claims Service of the Bank of Spain

María Luisa García
Head of the Bank of Spain Claims Service

Introduction

The evolution of the financial systems of all developed countries has reached a degree of maturity that will allow us to successfully implement new economic systems based on the latest technologies. This will result in growth of all economic sectors, with changes in the social structures themselves, consumer habits, the spending decisions of national economies, investments by companies and governments' economic policies.

Impact of fraud on the European market

This evolution is evident within the European Community, the core of which is the Single Market.

Over its more than 12 years of existence many directives and recommendations have been issued affecting the legal systems of the Member States. The opening of the various national markets is an ever more palpable reality. The objective of free movement of goods, services, persons and capital, with the

elimination of the technical barriers imposed by the various protectionist policies, is a fact.

For all of these reasons it is urgent to respond to current economic and social challenges and create a large European economic bloc, in order to consolidate the successes that have been achieved, eliminate such weaknesses as still exist (such as the lack of liberalization of financial services), and adopt specific measures (such as the creation of an integrated market for these services, the action plan for which was completed last year).

But protection is also required at another level. The elimination of barriers and free movement may be used for unlawful purposes in all areas of economic activity. In particular the new technologies and generalization of use of the Internet for commercial and financial transactions open new opportunities for the so-called "cyber criminals" to improperly obtain personal data, which they thereafter may use to engage in fraudulent transactions. It is obvious that this situation has a negative effect on the market, the use of trade and electronic money, and the protection of consumers, which are priority objectives of community policy.

Impact on consumer confidence

The strategy of the European Commission regarding consumer policy for the 2002-2006 five year period specifies achieving a high common level of protection as a priority objective.

To achieve this objective it is necessary to harmonize the economic and legal interests of consumers, so that they may undertake their transactions with the necessary confidence in any place in the EU. The Parliament has repeatedly emphasized the importance of having a maximum level of security for payment instruments, inviting the Commission to propose specific preventive measures.

The loss of confidence of European consumers resulting from the increase in levels of cross-border fraud, more so than national fraud, which to a large extent affects remote payment transactions, principally using the Internet, gives rise to insecurity in the proper functioning of the financial system, impeding the potential growth of e-commerce.

An efficient financial system assures healthy economic growth. But there is no efficiency without security. This requires those participating in the market to introduce the maximum level of technical security that is viable from an economic point of view.

Fraud in financial institutions

The bank fraud that most affects consumers is fraud related to transactions effectuated through electronic banking.

Criminal organizations, often operating in different countries within and outside the Union, engage in ever more sophisticated and complex attacks, with periodic appearance of new methods that require adoption of measures by the banking industry, telecommunications operators, governments and community organizations, in order to adopt an overall view of prevention of this kind of crime.

Bank fraud using the Internet

The volume of transactions engaged in using the Internet, the extension of online banking services and the wealth of information that ultimately is available on the Web facilitate bank fraud, which sometimes is of an alarming size.

Such fraud is based on "identity theft," by means of which personal data and passwords are accessed and later used for fraudulent purposes.

The forms of these illegal captures of data may reach high levels of sophistication.

The best-known systems are the so-called "phishing" and "pharming" which fall within the techniques of social engineering.

In phishing, a false e-mail is used. It pretends to come from a bank. It directs the user to enter personal passwords. This having been done, they are captured by the computer pirate. One of the most common forms of fraud is the use of these passwords to make transfers from the victim's bank account to the account of an intermediary. From that account the funds are transferred using any of the international agencies for sending transfers.

In pharming, the pirates manipulate the DNS (domain name) addresses. The result is that the Web pages of the banks are replaced by other false pages for collection of confidential data.

In both cases access to the victims' computers is achieved by introduction of "malicious codes," called Trojans, that incapacitate the computer's security and destroy or modify data.

Fraud with credit/debit cards

The fraudulent use of cards may be accomplished in several ways, from theft or robbery from the holder and later use in transactions or ATMs, to cloning the

plastic, obtaining the codes hidden in the magnetic stripe and recording them on a new card for use thereafter for fraudulent purposes.

The greatest risk facing a cardholder is cloning, because the holder does not lose possession thereof and therefore is not aware of the improper use by the defrauder until it receives notice of the expenses or withdrawals that have been made. For this reason the amounts drawn may reach significant amounts.

Personal passwords may be obtained in many ways. These range from the simple, such as installation of hidden cameras at ATMs, or observation by the criminal while the victim is using an ATM, to the use of a card reader, called a "skimmer," similar to those installed at entrances to ATMs, with capacity to store a large number of passwords and capture information by just swiping the card.

Measures to be adopted by financial institutions

Financial institutions may play a significant role in prevention and detection of bank fraud.

The Centre for Interbank Cooperation has a computer security group responsible for considering measures to be taken to combat fraud by the financial institutions operating in Spain.

Three large groups of measures may be identified for adoption by financial institutions.

Measures for computer security in their own systems, preventing improper access thereto.

Technical measures, such as the establishment of more secure user access controls, for example by using tokens generating passwords, use of digital certificates, chip cards, digital national identity documents (DNI), secure webpages, use of public key algorithms, etc.

Another kind of measure is organizational: bank contracting policies, on the order of "know your customer," training, educating electronic banking clientele regarding the risks of not properly protecting their computer equipment, sending encrypted text messages to customers, alerting them of certain transactions, or introduction of contractual clauses allowing blocking access to the electronic banking service when there are indicators of irregular transactions.

New European measures in combating fraud

Public and private institutions, national and community, as well as consumers and users, are concerned by the lack of security and privacy that hinders development of the Information Society and, therefore, negatively affects e-commerce.

The trends to convergence of identification and authentication instruments, and the use of technology strengthening privacy, with maximum limitation of the collection of personal data for undertaking commercial or financial transactions, may have negative effects on security, and make identity theft easier.

The goal of a Single European Market, eliminating barriers that prevent free movement of goods, services, persons and capital, implies interoperability of the various systems.

Protecting the financial interests of the Community is fundamental. Preventive measures to combat fraud and falsification of means of payment other than cash are a priority objective.

In February 2001 the Commission approved the 2001-2003 Action Plan for prevention of fraud and falsification of means of payment other than cash. This was intended to confront the disturbing growth of fraud and falsification, 50% in 2000, and its greater impact at the cross-border level. The personal information travelling over the web for purposes of collections and payments must be secure.

Cooperation of all interested parties and strengthening the security of payments were established as fundamental principles.

Most of the actions contemplated in the plan were successfully implemented.

In order to continue its actions in this regard, the Commission adopted a new Action Plan for 2004-2007. The priority areas will continue to be security of payments and improved cooperation among public authorities and the private sector.

Among others, the following were established as specific measures:

— Identification of fraud prevention experts in each sector to act on a coordinated basis.
— Improving transparency of the procedures for development of security and promoting standardization.
— Providing citizens with more complete and clear information regarding the security of the payments they make.
— Improving the system for giving notice of loss and theft of payment cards in the EU.

— Adopting specific initiatives intended to prevent identity theft.
— Commencing a study of the methods of verification of holders with respect to card payments and users with respect to electronic and mobile telephone payments.
— Without abandoning respect for the rights and freedoms of persons and the competition rules, the interested parties must be able to interchange information for early detection and notice of attempted fraud. The Internet page of the EU regarding fraud prevention could become a point of reference accessible to citizens, companies and governments.
— Strengthening the work of the EU's Expert Group (FPEG), created by the Commission as a part of the 2001-2003 Action Plan. This group of experts includes representatives of all the parties involved in the problem, working in various subgroups. Its purpose is to prevent card fraud and Internet payment fraud.

The specific matters on which it is working are:

— First a study, and then recommendations for the member countries to harmonize their systems for evaluation of the degree of security of payments.
— Evaluation of current security measures applied to transactions at ATMs and point of sale terminals. The purpose is to achieve better cooperation among banks, businesses and customers, to make the measures adopted more effective.
— Analysis of the systems used for identity theft, proposing recommendations and actions to prevent it.

One of the most important measures that is being studied, having greatest impact on privacy, is the viability of creation of a database of frauds that are discovered. This was suggested by the European Council within the proposal of a Means of Payment Directive.

In order to assure compliance with the Personal Data Protection Directive, work is being undertaken in collaboration with the "Article 29" working party, which assists the Commission on matters related to data protection.

Finally, the legal barriers existing to interchange of data among those in the public and private sectors involved in combating crime will be studied, as will possible means of eliminating them.

The Data Protection Authorities Committee of the European Union (article 29 Working Party) approved guidelines to be followed regarding data collection

and processing by businesses whose payment card acceptance agreements have been rescinded, without including data regarding individual holders. This is intended to assist in preventing fraud and assure that the privacy of businessmen is better protected. This measure is considered to be very positive, as an example of the balance between respect for the fundamental rights and freedoms of persons, having the right of privacy, and their proper application to security and proper functioning of financial services. It is necessary to assure proper use of data, exclusively for the indicated purposes.

The Commission and the data protection experts have negotiated these guidelines with VISA Europe and MasterCard Europe, establishing the objective criteria that may be used to include the names of businesses whose agreements have been rescinded and may be involved in fraud.

The success of these measures will depend on a series of factors and the degree of involvement of the participating parties, both institutions and individuals. It is important that the degree of awareness of the problems we confront be high, that consumers be aware of the risks they assume by not adopting appropriate security measures in their transactions, in short, not trading privacy or security for convenience.

Finally, we must promote cooperation between the public and private sectors, principally banks, because the private sector has the most developed preventive technology, promoting the installation of new systems that increase security.

Creation of a single payment area in the European Union

The measures adopted by the Action Plan to combat fraud are complemented by the new Means of Payment Directive, currently being studied. It is intended to achieve the objective of creating a Single Payment Market, within which the maintenance of secure and effective payment systems is essential.

The system concentrates on electronic payments as an alternative to cash payments, which are much more costly. In order to promote their use it is essential to have limits of liability in the event of unauthorized use of such payment instruments as have been stolen or lost, with that circumstance having been communicated to the service provider, establishing more detailed rules regarding fraudulent use of payment cards.

The proposed directive, as we have noted, proposes efficient interchange of data among payment service providers, which must be allowed to collect, process and interchange the personal data of all those involved in this kind of fraud, re-

specting the provisions of Directive 95/46/EC of the European Parliament and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Protection of personal data

In Europe the protection of personal data is regulated by Directive 95/46/EC of the European Parliament and of the Council, incorporated into our national legislation by Organic Personal Data Protection Act 15/1999 of 13 December 1999.

Effectively implementing the protection measures discussed above will result from reaching more homogeneous application of the Data Protection Directive in national legislation within Europe, in such manner that situations do not occur where the communication and transfer of information is not possible.

The objective is ambitious but not impossible. European citizens must feel secure in their transactions, and at the same time maintain their privacy. In turn, respect for privacy may not be used as an argument for not providing the information necessary for identification and prevention of fraud.

But it is necessary to maximize the measures assuring that the databases containing information regarding those participating in bank fraud will be appropriately managed as regards respect for the privacy of those involved, in such manner that doubts do not arise regarding protection of their fundamental rights.

This problem is of greater significance in relationships with third countries whose legislations regarding data protection may be different from ours. Therefore, the Commission proposes the adoption of measures to raise awareness regarding fraud in those countries, cooperating in multilateral forums such as the G8 in order to combat it.

The experience of the Claims Service. Background

The Claims Service received the first reports of improper use of credit cards in 1988. At that time the security systems of the various institutions were not interconnected. After notice of theft or loss of a card, blockage occurred only at the ATMs of the issuing institution. It could not be used at the ATMs of other institutions.

Faced by these reports, the position of the Bank of Spain was that the institutions were responsible for the functioning of a system the risks and limitations of which were known only to them. It did not permit contractual clauses disclaiming

liability, and characterized such actions as contrary to good banking uses and practices.

Later developments

By reading the annual reports of the Claims Service one can see the development over the following years of the reported problems.

Cases of violation of the Code of Good Conduct for European Banking began to appear in 1991 as regards the Card Payment Systems of 14/11/1990, responding to the European Recommendation regarding payment systems 88/590/EEC. The liability of the cardholder in the event of fraudulent use, prior to notice to the issuing institution of loss or theft, was limited to 150 ecus, now euros.

Incorporation of this limited liability into contracts occurred on a progressive basis. Currently it is a part of almost all of them. Some even include lower limits.

The problem was evolving. Cases were reported of return of allegedly fraudulent transactions to businesses, despite undertaking the transaction with physical delivery of the card, and apparent matching of the signature with the one on the corresponding invoice.

With the introduction of e-commerce, cases appeared of returns of transactions undertaken by using the card number on the Web, thereafter rejected by the cardholder.

Finally, the cases presented cantered on alleged cloning of the plastic and fraudulent use.

The following table shows the number of claims presented for improper use of cards. The greatest growth is during the years 2001-2002

The following graph shows the specific ratios to all card claims and all claims.

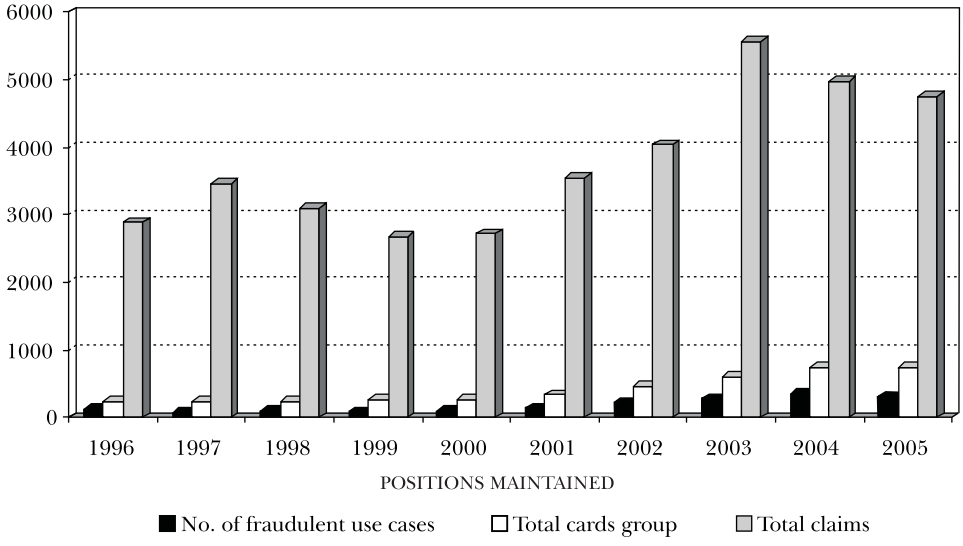
The Claims Service has been insisting that financial institutions must use all resources available to them to assure proper functioning and security of the system and that, in those cases in which defects appear therein, they may not transfer the negative consequences to banking customers.

The application of the limitation of liability has always been deemed to be necessary from the point of view of good banking practices, and failure to apply it, invoking negligent actions by cardholders, requires analysis of the specific case which, ultimately, requires a judicial decision regarding the matter in question.

For all of these reasons, automatic classification as "lack of diligence," based merely on the fact that the fraudulent use of the card has been undertaken using the correct personal identification number (PIN), and that this implies lack of

Year	No. of cases	% of group (1)	% of total (2)	% Growth
1994	88	41.12	3.47	
1995	104	46.64	3.84	18.2
1996	124	49.6	4.29	19.2
1997	69	29.24	1.99	–44.4
1998	104	41.43	3.35	50.7
1999	92	34.46	3.44	–11.5
2000	103	36.92	3.79	12.0
2001	143	41.57	4.03	38.8
2002	231	49.25	5.72	61.5
2003	283	46.85	5.08	22.5
2004	347	47.02	6.97	22.6
2005	311	41.97	6.54	–10.4

(1) Percentage of total card claims.
(2) Percentage of total claims.



care by the holder, is not permitted. This is because it has been shown that these personal identification numbers can be obtained in a variety of ways, such as the possibility of cloning the cards for their fraudulent use.

Case law regarding this matter is extensive, and also has evolved to the point of admitting the possibility of using sophisticated technical resources to verify the

personal identification numbers (PINs) on the cards, applying the doctrine of risk to the card payment system and, therefore, making the issuing institution responsible for showing that the system is secure and infallible.

In short, the Claims Service is aware of the seriousness of the problem of insecurity of electronic means of payment, and the need to protect the financial consumer. Therefore, through its reports it warns consumers of the risks they assume through their negligent use, providing alerts by means of the information offered on the Bank of Spain's Web page of the most common means of attack for capture of personal passwords, and encouraging users of electronic banking to adopt appropriate computer security measures to protect their equipment.

Current situation

New problems have been recognized by the Bank of Spain, through claims presented or messages sent to the e-mail addresses available to consumers.

There have been reports of frauds of various kinds using false sales over the Internet, many cases of phishing, false e-mails from financial institutions advising of false lottery prizes, and requiring that funds be sent to a bank account before collecting the prize.

The Claims of Service has been advised of problems of identification of beneficiaries of transfers sent through currency exchange and transfer establishments that sometimes are used as the last link in the fraudulent chain, as they have no obligation to retain the documentation presented at the time of payment, thus making it more difficult to identify the person that withdrew the funds which, in addition, in many cases occurs in countries outside of the Community.

To summarize, the Claims Service of the Bank of Spain is a direct observer of the degree of the public's awareness of problems that worry all of us. All of us, to a greater or lesser extent, are involved in the solution.

16

New European Proposals in the Battle against Fraud in the Financial Sector and their Effect on Privacy

Honorio Ruiz
General Secretary of the National Association of Financial Lending Institutions

I thank the Spanish Data Protection Agency, the BBVA Foundation and the Superior Council of Chambers of Commerce, Industry and Navigation for their invitation to me as Secretary General of the National Association of Financial Lending Institutions, to discuss what financial institutions in some countries of the Union have proposed to combat fraud in economic and financial activities, and in particular to report on what we are currently doing in Spain, which in truth is a novel European proposal because it has been created on the basis of the Spanish legislation on protection of personal data. I believe the solution we propose may be a valid instrument for other European countries that have legislation regarding data protection comparable to the Spanish legislation.

I would like to begin with a reflection. The financial sector of western countries that respect the privacy of their citizens is being attacked, as has always been the case, by falsities regarding identification and solvency, both in traditional financial transactions and in transactions undertaken using the new information and telecommunications technologies (ICT). But what is really serious currently is that the most significant attack does not come from individual criminals, but rather from organized groups that have determined that they can obtain easy

money by deceiving the risk analysis departments of banks, savings banks and financial lending institutions.

Western financial systems always will be exposed to occasional serious blows from financial crime. But what really may harm them is generalization of small frauds fundamentally tied to consumer finance transactions.

In Spain financial institutions for some time have been aware that they must change their current business practices for consumer financing, introducing preventive measures therein that heretofore would have been unthinkable from a commercial point of view. They also are aware that they cannot combat fraud on an individual basis, without strengthening cooperation among undertakings. For this purpose they need to pool the negative information held by each of them deriving from transactions that prove to be irregular and, therefore, presumably fraudulent.

If the European financial institutions do not themselves take measures against fraud, surely they will soon be imposed by their respective supervisory authorities.

But within the European Union any proposal for the financial institutions to share sensitive information, because it necessarily affects the privacy of citizens, must respect the applicable laws regarding protection of personal data. It is for this reason that the domestic legislation of each country is placing conditions on the common tools that the financial institutions may use against fraud.

I am referring to common tools for the financial sector because, within the internal operations of each institution, internal and external tools have always been used for risk analysis and to prevent delinquency (databases, "scoring" programs, delinquency files, programs to integrate information existing in the market or expressly created for the purpose by specialized companies). There is very little experience in Europe regarding transfer of data among companies for the fight against fraud. The most significant examples of which I am aware are as follows:

In Europe:

— The UK's Fraud Prevention Service (CIFAS).

In the rest of the world:

— Federal Trade Commission;
— Association of Certified Fraud Examiners, an international organization with offices in some European countries;

— Cooperation since 2004 between Equifax-Uruguay and the Ministry of the Interior of Uruguay.

In the insurance sector there is a European tradition of cooperation of companies. For years this has permitted the creation of many anti-fraud databases in a large number of the countries in the Union. In Spain the insurance legislation allows creation of common anti-fraud databases.

If you allow me I will give some brief comments on the experiences referenced above.

The UK's Fraud Prevention Service (CIFAS)

The United Kingdom Fraud Prevention Service was created in 1988 by consumer finance lending institutions. It is an association that is dedicated exclusively to the prevention of financial crime.

CIFAS provides a range of fraud prevention services to its members, including a "system or database" that is being used by most financial services companies.

The government and the member companies are represented in the association, providing coordination and training, as well as a communications network for all members. The members are not only consumer credit companies, but also banks and credit card, telecommunications, factoring, insurance, mortgage, electricity, and fund management companies, among others. CIFAS grew rapidly in the following years, and became an independent company on 22 February 1991.

The purpose of the association is to protect the interests of the CIFAS members against actions of criminals, collecting information regarding frauds that have been consummated and those that have been avoided, and assuring that the improper use of identities does not harm the citizens that are victims of fraud. The documentation is shared in the public interest between the public and private sectors. The CIFAS services, therefore, are not offered only to members, but also to the general public, helping protect consumers against identity theft.

CIFAS for years has been providing a model for properly sharing information among companies and protecting privacy rights as required by British law.

The quality of the data is the responsibility of the institutions that populate the system databases with all detected cases of fraud. The system generates alerts for the entities that reciprocally interchange information.

Federal Trade Commission

This is a federal agency of the United States government, created in 1914. Currently it is engaged in educating consumers and companies regarding the importance of privacy of personal information. For that purpose it issues many publications.

The Federal Trade Commission works particularly for consumers in the prevention of fraudulent, deceptive and unfair business practices, and to provide useful information for the identification, prevention and avoidance of such practices. It collects complaints from victims of identity theft and shares its information with authorities throughout the country.

This information may also be shared with other governmental agencies, consumer reporting agencies, and companies where frauds have been perpetrated, with the purpose of collaborating in resolution of the problems related to identity theft.

The Commission has some 1000 members, of whom 500 are lawyers and 70 are economists.

Association of Certified Fraud Examiners

The Association of Certified Fraud Examiners is dedicated on an international scale to training of various professionals who, in their companies or organizations, are engaged in combating fraud. Among them are internal auditors, accountants, attorneys, fraud investigators and police force personnel. In this regard it cooperates with many universities. It generally grants its own certificates to students who pass the various courses it plans.

It therefore is a good international observatory for fraudulent activity, because each year it analyzes thousands of fraud cases and is a good international network for operational connection of specialists.

In January 2004 a cooperation agreement was signed by the Ministry of Interior of Uruguay and the Equifax company in that country. It is called "Clearing de Informes" ["Report Clearing"]. The purpose is to provide the public with a means of reporting theft or loss of identity documents using a 900 service, in real time, from home or the place of the occurrence.

This service is in operation 24 hours per day throughout the year, with a fixed cost per call. Within the 24 following hours the citizen is sent the report form corresponding to the domicile provided by the citizen.

Through use of this procedure, the information is immediately made known to the financial and business institutions by means of a database. The purpose is to prevent the damage that is caused by use of stolen or lost identity documents.

In the European institutional framework, the authorities of the Union are very aware of the fraud problem in the financial sector, supporting cooperation between the private and public sectors, as shown by:

a) The Notice of the Commission to the Council and to the European Parliament regarding the prevention of and fight against organized crime in the financial sector of 16 April 2004, stating the necessity of cooperation between the financial and business sectors and the security forces of the state on a communitywide basis.
b) The Framework Decision of the Council of 28 May 2001 on the fight against fraud and falsification of means of payment other than cash, contemplating cooperation among public and private services and agencies responsible for management, control and surveillance of payment systems, and with the national authorities responsible for investigation and prosecution of violations.
c) The creation of the European Anti-Fraud Office (OLAF) itself. Its mission is protection of the interests of the European Union, combating fraud, corruption and any other irregular activity, including the irregularities of European institutions. This institution was created in 1999. It performs its mission with total independence in its internal and external investigations. It cooperates with the competent authorities of the Member States, which it assists and supports in their antifraud activities.

Within this set of agencies that the European Congress dedicates to the fight against fraud and protection of data, some of them identify a part of the problem that the financial institutions must promptly resolve. If you will allow me, I would like to offer a brief description of the problem we are experiencing within Spanish financial institutions:

Currently, using the same falsified identities and solvencies, various financial institutions throughout Spain are being attacked on a simultaneous basis. The criminals in their fraudulent activities are taking advantage of the fragmentation of information within the financial sector, and even the operational dispersion of the security forces themselves.

The financial activities that on a general basis are most affected by criminal activity are those dedicated to consumer finance.

The appearance of this fraud in our financing transactions is what motivated the Association in 2002 to create the Fraud Prevention Service, to promote operational coordination of our institutions in prevention of and reaction to fraud. The Service was formed as a means of monitoring the fraudulent activity suffered by the financial sector, and to provide technical advice to the Commission for the Prevention of Fraud, on which the institutions belonging to the Association are represented, and has been functioning for a number of years.

During following years, within the Association we have worked internally to give Spanish financial institutions new anti-fraud tools, and to increase cooperation in this regard with the public authorities. This is because we are convinced that only by means of operational coordination among institutions and decisive cooperation with public institutions can we stop the current crime against the financial system.

We have signed cooperation agreements with the Ministry of Interior, with Interior departments and with the Catalan and Basque governments, and with the Superior Council of the Judiciary.

Our work over these years has raised awareness of this matter throughout the sector, to the point that currently other initiatives are arising within financial institutions, which are following the same path we have followed for some years. This makes us very proud.

Allow me to offer some figures to help assess the problem:

In 2005 consumer finance fraud in Spain amounted to an estimated 260 million euros, 16% more than in 2004. These figures do not include the fraud we have managed to stop using operational coordination among our companies. Considering only the institutions that are members of ASNEF [the National Association of Financial Lending Institutions], in 2005 it is estimated that they suffered 76 million euros of fraud, of which more than 90% affected the financing of automobiles, with an average per vehicle of some 30,000 euros. We are working to obtain more precise fraud statistics not related to automobiles using computer applications that we have installed. For this lesser area of consumption our sample is not sufficiently representative.

To deceive us, the organized crime groups working to defraud our financial institutions are using:

1. Impersonation of true identities.
2. False identities created based on authentic documents, modifying some of the information.
3. Totally invented identities.

4. They also are using marginal individuals that use their own identities for a price.

In all cases, these criminal organizations provide the persons working with them with the solvency documentation necessary for the fraud, in the same way as is done by individual perpetrators of fraud that use their own identities.

Because to date it has not been possible to reciprocally transfer negative information among institutions, each of the false or falsified identities created by the organized groups has been used on a simultaneous basis in several financing transactions in the same or different cities, thereby multiplying the damage to the institutions.

Although the financial institutions are increasingly conscious of the need to report frauds, even though that represents a cost in addition to the loss that is incurred, police and judicial actions prove to be ineffective because consumer frauds normally are small in amount, which results in the police investigation generally not being coordinated and focused. Therefore each case is handled on a decentralized basis throughout the country by different police units in different courts, with the resulting waste of resources of public authorities and the victimized companies.

But there is even more. In the fraudulent consumer finance transactions the first victims are the financial institutions that are economically harmed by these frauds but often there is a group of citizens that are particularly victimized by the criminals: the true owners of the identities that are used in the fraud.

According to official statistics of the national police force for 2003, 474,729 national identity documents were lost and 489,222 were stolen. That is, lost and stolen documents in 2003 totalled 962,951. There were 14,448 Spanish passports lost or stolen in the same year. If to this number we also add the lost or stolen residence cards of foreigners, and those for which we do not have information, we may believe that in that year nearly a million and a half Spanish identity documents may have been used for illegal purchases and sales on the criminal black markets. And we are only talking about the statistics of the national police force. So if we had specific information regarding statistics on lost and stolen documents from the Civil Guard, the Mossos d'Esquadra [Catalonia police force] and Ertzaintza [Basque police force], these figures would be even higher.

With these numbers of lost and stolen documents in the hands of criminals we can easily understand the seriousness of this problem and what it will mean in the future regarding proper functioning of the financial business. We all know that the financial system is a very efficient structure if it operates with properly identified

citizens who therefore are properly monitored regarding possible delinquency. But the system is very vulnerable if criminals with false identities are introduced into it.

The current situation is resulting in serious damage to financial institutions and, therefore, to all credit activities but also for the public authorities because they must dedicate a part of their scarce resources, police and judicial, to investigations that arise with insufficient information, often remaining unresolved. But in my opinion it is the citizens whose identities are used who are most unjustly victimized. Even if they report the loss or theft of their identity documents at the time, use of their identities by the criminals causes damage to their honour and assets that often is very difficult to repair. This is because they generally are often summoned by the police or judicially, causing personal and professional loss. They are inconvenienced at the borders or by reason of hotel security when they travel or they are deprived from the outset of access to credit in the financial system because their names are entered in the delinquency databases.

Unfortunately in Spain to date there has been no solution, public or private, allowing citizens to preserve their identity within the financial system in the event of loss or theft of their identity documents. But I can advise you that since January of this year the solution exists. It has been created and implemented by the financial institutions themselves through *Servicio Veraz [Truthful Service],* which our institutions have joined and which is demonstrating its true usefulness.

This Service is open to all financial institutions, even if they are not members of the Association, thus respecting the Defence of Competition Legislation.

I will not bore you by explaining its structure and functions. But if anyone is interested you need only ask our Association or go to its website: www.verazspf.es

I will simply note that the Service currently is comprised of three databases that may be populated automatically and manually. They generate alerts when accessed by the companies' search engines. But the detailed information they contain may only be viewed by certain departments of the companies specialized in fraud prevention, so that the information will be appropriately used, respecting privacy. Within each company there is a person that internally oversees compliance at all times with the code of ethics or regulations regarding these databases, the use of which is also monitored externally by a committee.

Each of the databases contains its own information.

One of them, called VERAZ-FODI, is a database based on reciprocity, populated by all of the institutions based on contradictory data from their own financial transactions, the transfer of which is justified to the Spanish Data Protection

Agency using a support file containing the internal investigation made to verify the truth of the data, as well as such documents regarding enforcement of rights as may be specified by Spanish data protection legislation.

The second database is called VERAZ-SOCIEDADES. It is filled by public sources, Borme [the Official Gazette of the Commercial Registry] and judicial information advising of companies in bankruptcy, being extinguished, that are inactive, etc.

And the third, called VERAZ-PERSUS, which is made available to all citizens that lose their documentation or have it stolen and wish to include themselves to preserve their identities within the financial and business system, and thus prevent conduct prejudicial to them and their assets deriving from their impersonation to engage in credit transactions, obtain credit cards, personal loans, the opening of false bank accounts, remote purchases and sales, and many other criminal activities.

This database may be populated by citizens by means of:

1. Self inclusion, or direct inclusion by the citizens involved themselves, using the computer system we have created. This self inclusion may be accomplished by using the system operator, various public and police agencies (we are working to sign the necessary cooperation protocol), and the financial institutions participating in the Service themselves, which may arrange for self inclusion of their own customers and thereby offer them a new service.
2. Indirect inclusion by the citizen himself through the mail, customer service offices and such entities as may determine that they will use the direct inclusion system.
3. Inclusion by legal guardians using the means referred to above: parents, relatives with legal representation and public entities responsible for dependent persons.

In conclusion I would like to offer a reflection on the aspects of the Service that affect the privacy of data, and which I believe are of most interest for purposes of this presentation.

From the outset of the project, those responsible believed that its legal configuration would be the cornerstone for the entire structure, since the success or failure the Service could depend on compliance with the data protection regulations.

For this reason, the legal team of *Equifax Ibérica* and representatives of ASNEF began to hold conversations with the Spanish Data Protection Agency. From the

first meetings it could be seen that it would be necessary to structure the Service and therefore the operation of the VERAZ-FODI and VERAZ-PERSUS databases on the basis of the following principles:

1. Consent of the interested party, both for consultation and for inclusion of that party's data in the databases.
2. Full respect for exercise of the rights of access, rectification, erasure and opposition by interested parties.
3. Creation of Regulations or a Code of Ethics of mandatory compliance by the institutions using the Service.

Once these three principles had been adopted, the indicated work culminated with presentation of regulations for the Service on 28 October 2005, for non-binding review by the Spanish Data Protection Agency, the only mechanism contemplated in the Organic Data Protection Act and its complementary provisions.

The purpose thereof, even knowing that the response would not be binding, was to have the opinion of the Spanish Data Protection Agency regarding the operation we wished to offer, in addition to having its supervision in order to avoid taking an improper path that in the future could result in sanctioning proceedings or suspension of the Service.

On 17 February 2006 we received from the Spanish Data Protection Agency the answer and report that allowed us to conclude that, by fully respecting and complying with the rules established in the internal Regulations of the Service controlling the reciprocity database, it will be consistent and comply with the Data Protection regulations.

The Regulations of the Service include consent clauses that will be used by the institutions as documents separate from the application or contracting forms for transactions, which must be signed by the interested parties, providing them with the opportunity to state their refusal to allow processing or transfer using a simple procedure, that being marking a box for that purpose. As a result a procedure is established for collecting the express written consent of those involved, who may state their refusal to allow processing and transfer of their personal data. The regulations also provide that refusal to allow consultation or inclusion of the data in the reciprocity database cannot justify denial of the transaction requested by the interested party.

The institutions are required to retain the documents containing the informed consent, and to prepare a verification file before transferring data to the

database. That file must contain the consent document and the other documents regarding exercise of rights.

Regarding the reciprocity database, the Regulations for the Service properly describe it as the most complicated from a legal point of view:

1. The purposes of the database, the data that will be included therein or that will be consulted, all of them related to detection of irregular transactions or transactions with inconsistent data, which constitute its purpose, the identification of the kind of business of the creators of the database and, therefore, the transferees of the data, and the manner in which the rights of access, rectification, erasure and opposition may be exercised.
2. It also imposes an obligation on the participating institutions to prevent use of the content of the database for any purpose other than those contemplated in the Regulations.
3. To assure the accuracy of the data transferred, within each institution a position of spokesman or coordinator is established. That person is responsible for reports regarding verification, with the results of the comparisons undertaken, detailing the procedure for verification of the inconsistent information in the credit application, the date it was known to the user institution, the source or means of obtaining the information, as well as the documentation showing the untruthfulness or irregularity of the information or documentation provided. The file must reflect exercises of the rights of correction, suppression and opposition, properly regulating their exercise by citizens.
4. To even further assure privacy, the Regulations establish a regulated procedure for consultation, and specify that personal data will be suppressed when they have ceased to be necessary or pertinent to the purpose for which they were collected or entered, and in any event will not be maintained for more than six years after the first inclusion of personal data in the database.
5. The Regulations properly specify the responsibilities of the Data Controller, the Controller and the institutions using the Database, as well as the security measures specified by the data protection legislation.

I would like to refer briefly to two initiatives that also have been implemented by ASNEF, and that we hope soon will be instruments for prevention of fraud in the financial and commercial sector:

1. One of them is the possibility of online verification against Social Security databases of information provided in that regard by an applicant for credit, financing or a financial lease.
   The verification will require prior express written authorization of the applicant, and will be limited to confirming or denying the truthfulness of the data provided. It may not be subject to later processing by either Social Security or the credit institution, it being required to immediately destroy the information.
   The verification system would be similar to the one established for consulting the Risk Centre of the Bank of Spain.
   Currently this initiative has become a bill to amend Article 66 of Royal Legislative Decree 1/1994 of 20 June 1994, approving the Consolidated Text of the Social Security Act (Official Gazette of the Spanish Parliament of 11 June 2004).
2. ASNEF also is working on a novel project called DELFIN *(delitos financieros*—financial crimes), the goal being an agreement between public and private institutions for the creation of a virtual office for reporting crimes committed in the context of credit, financing or financial leasing transactions.
   This initiative would allow effective cooperation of financial institutions with investigating judges and security forces to combat the organized crime that is acting against the financial sector. At the same time it would allow creation of an intelligence system that would interrelate the criminal acts committed with the identities themselves, which would serve to optimize judicial and police work.

I believe that financial institutions have decided to take a step forward in prevention of fraud, with no fear of the personal data protection legislation existing in Spain, making a great economic and organizational effort to adapt their internal business procedures and thus comply with the regulations of the new Service.

We wish to publicly thank our Data Protection Agency for its patience with us over these years, and its confidence in the financial and commercial sector of Spain being able to create such a novel and complex Service, but in accordance with the provisions of Organic Act 15/1999.

17

The Fight against Fraud in Europe and the Protection of Personal Data

Laraine Laudati
Chief Administrator of the European Anti-Fraud Office

Thank you to the organisers of the conference for the invitation to speak today. I think that it has been especially important that the organisers have managed to assemble various perspectives on the problems of data protection, presenting the views from both the public and private sector. Enabling this kind of exchange of views is what helps us all to understand each other and the problems that we're facing, which I think is extremely valuable.

I'd like to begin my talk with a brief description of OLAF and then to address two or three of the major aspects of data protection that we are dealing with within OLAF.

"OLAF" is the French acronym for the "Office Europeen de Lutte Antifraude," in English the European Anti-Fraud Office. We are responsible for investigating fraud against the financial interests of the European Union. Fraud may occur in the context of the distribution of vast amounts of EU funds by the Commission and the Member States in the form of structural funds and development funds. It may also occur in the collection of customs duties, as well as the Common Agricultural Policy and in the anti-dumping area.

OLAF was created in 1999 to achieve the objective of conducting investigations for the fight against fraud which harms the financial interests of the EU.

These include internal investigations, (those focusing on the officials and other servants of the EU institutions, agencies and bodies), as well as external investigations (administrative investigations outside the Community organs for the purpose of detecting fraud or other irregular conduct of natural or legal persons). Internal investigations are a particular priority of the Commission, which has a policy of "zero tolerance" in relation to suspected fraud, irregularities and corruption within the EU institutions. OLAF also plays a pivotal role in coordinating the activities of member state authorities that are involved in investigations for the fight against fraud involving EU funds.

Upon the conclusion of an OLAF internal or external investigation, OLAF produces a final case report, which contains OLAF's conclusions with respect to the fraud under investigation, and of course, normally contains sensitive of personal data. The final case report of an internal investigation is transmitted to the EU institution concerned, and if there are possible criminal aspects, it will also be transmitted to the appropriate criminal authorities in the Member States. Each of those authorities will be responsible for follow-up action. The final case report of an external investigation will be transmitted to the EU institutions and member state authorities that will be responsible for follow-up. The follow-up in the external investigations may also include criminal proceedings.

All of the information gathered by OLAF is subject to the professional secrecy rules of the Community, which are set forth in the EC Treaty and the staff regulations. These rules would, nonetheless, allow for certain disclosures of the information, such as the transmission of the final case report to the authorities responsible for the follow-up as established by the OLAF legal framework. All of the rules related to both confidentiality and professional secrecy and the distribution of the results of OLAF investigations, as well as all other procedures that we follow, are thoroughly described in our OLAF manual which is what our investigators are obliged to follow in their handling of the information that they gather.

I will now turn to the data protection aspects that I would like to discuss. First, we are in the world of Regulation 45/2001 and not the Data Protection Directive. They are very closely parallel, but there are certain differences. All of the EU institutions are obliged to implement the Regulation. Thus, in performing its investigation functions, OLAF obviously processes large amounts of very sensitive personal data, and this must be done in full compliance with the Regulation.

The data protection officer plays a crucial role in this regard, in close cooperation with Mr. Hustinx, who was here yesterday talking about his role as the European Data Protection Supervisor. The Commission has two data protection officers: one for most of the Commission and myself, the data protection officer for

OLAF. The reason that OLAF has its own data protection officer is that, in performing its investigation functions, it must operate in complete independence. Since most of the personal data that it process relates to investigations, it must have a separate data protection officer.

Information to the data subject

The regulation, of course, provides in Articles 11 and 12 that certain information must be provided to the data subject, but this is very difficult to imagine for an investigation authority that is conducting investigations of fraud, where it's not usually convenient to provide information to those who are the subject of the investigation, at least during the course of the investigation. And so how can we act in accordance with the regulation's requirements in this regard? There is an exception that is provided in Article 20 of the regulation, which allows for delays in the application of certain provisions, including this article on informing the data subject where it would be harmful or where it's necessary to do so to safeguard the interests of prevention, investigation detection and prosecution of criminal offences. Not all OLAF investigations involve criminal offences, but in any event, this provision is read rather broadly so that it might include investigations where criminal offences are not at issue. But there are several other exemptions that also apply, such as important economic or financial interests of the Member States or of the EC, as well as protection of the data subject or the rights and freedoms of others. Thus, OLAF would normally be exempt from the requirement to inform the data subject in the course of an investigations.

OLAF's legal framework provides for informing the data subject who is the person concerned in an internal investigation when it becomes apparent that he is concerned, provided that doing so would not harm the interests of the investigation. OLAF must often defer the notification until a later point or the conclusion of the investigation. In exceptional cases, when it is necessary to maintain absolute secrecy, OLAF must defer the notification even after the investigation is closed. In the normal course of events, at the conclusion of the investigation, OLAF will provide the person concerned with the opportunity to present his views on all of the facts which concern him and so he becomes very aware of all of the information that has been gathered that is relevant to his personal data.

There is no right of access *per se* to OLAF's investigation file. As I've mentioned, we transmit our investigation results to the authorities of either the Member States or the institutions or both. During the follow-up procedures which they

conduct, access to the file is provided. In disciplinary proceedings, there is a specific provision of full access to the disciplinary file; in the national criminal proceedings, there are national criminal procedure for access to the file and that is how the access to the file requirements are satisfied. However, there is nothing in the legal framework of OLAF that provides for access to the file.

Transmission of information

Article 7 of the data protection regulation provides the rules for transfers of personal data within the EU institutions, or among the EU institutions. Article 8 provides the rules with respect to the sharing of personal data between an EU institution and an entity that is covered by the directive. Since our transfers are mainly to the institutions and the member state authorities, it is these two articles that generally govern our transmissions of operational information from a data protection perspective.

Article 2(g) of the regulation defines a 'recipient' to exclude someone that receives personal data in the course of an individual investigation. The transfer rules are thus, strictly speaking, not applicable to OLAF because we are transferring personal data in the context of individual investigations. Nonetheless, OLAF's transmissions fully satisfy the requirements of Articles 7 and 8. Article 7 specifies that the transfers within Community institutions are allowed if they are necessary for the legitimate performance of tasks, and we only transfer the information when it's necessary for the follow-up activities. Accordingly, we transmit information to the disciplinary authority so that it can carry out the disciplinary proceedings. Under Article 8, transmissions to member state authorities must be necessary for the performance of tasks carried out in the public interest or subject to the exercise of public authority. Even though, strictly speaking, the two articles are not applicable to our transfers in the context of investigations, we are fully in compliance with those articles.

Transfers to third country authorities are more complex. We are working to develop a system for transfers that will fully meet the requirements of Article 9 of the regulation. This may be in the form of a model memorandum of understanding.

Part v

DATA PROTECTION AND THE FIGHT AGAINST TERRORISM AND ORGANISED CRIME

18

Legal Instruments for Combating Terrorism

Juan José Martín Casallo
Deputy Prosecutor of the Supreme Court and Former Director of the Data Protection Agency

I wish to thank you for your presence, and of course also the BBVA Foundation, the Spanish Data Protection Agency and the Chambers of Commerce for giving me the opportunity to meet with you, some better known to me than others, and with old friends as I was reminded by the person beside me at this table.

In my presentation I would like to make one thing clear. It is personal and of course does not represent any official position, much less that of the Attorney General's Office, where I now work. Therefore what I say here is a matter of the personality and thought of Juan Martín Casallo. You are not to connect my personal thoughts with my performance of my duties. This is the afternoon. Let us say that my profession ceases when I leave it in the morning. I of course am opposed to terrorism. It is obvious, but sometimes it is appropriate to begin by making this statement. In the second place, I am in favour of any measure taken to combat terrorism, provided that the measure taken is of an exceptional nature and proportionate to the purpose of combating terrorism. That is, I am totally in favour of any interpretation that combats organized crime. I oppose all of it. I am in favour of eradicating it. I am in favour of implementing a series of police measures, provided that these police measures respect the criteria of proportionality with what is to be combated, and are by way of exception in the sense of

producing the minimum restriction of the fundamental rights of persons. It just cannot happen that in order to engage in the battle and assure ourselves of a fundamental right, we limit or eliminate four or five fundamental rights surrounding it.

The speaker preceding me, Rosa Díez, whom I admire from a distance because we are not personally acquainted, is right regarding the need to combat terrorism. But for me it is necessary to qualify this argument. Later, if I have time, I will give an example of what I want and am referring to. Thus what I am advocating is total judicial policy cooperation. Judicial policy cooperation, total. Combating any kind of organized crime, total. But always with the limitation, with the exception in time, of the proportionality of the measures taken and the existence of a supervisory authority limiting the actions of these forces, which normally and traditionally are inclined always to ask for more than they need, or to occupy more territory than they need. The purpose is to leave them in the proper place where, being effective in the fight, in this case against terrorism, they also are equally effective in continuing to maintain the fundamental rights of the European tradition that has existed over many years, specifically since the 19th century, recognizing the individuality of citizens. Therefore, I insist and I emphasize, no one is to conclude that I am against it, but always with the necessary limitations so that the right or rights we are trying to respect and protect are not eliminated by the protector we have appointed to defend us against the attacks that ultimately violate those rights.

This is the sense of police cooperation and judicial cooperation. That is, the sense of making matters more difficult for the terrorist organizations, thereby lessening their ability to engage in unlawful activities, their criminal activities, and therefore also so that we little by little, bit by bit will enjoy a greater degree of exercise of the content of fundamental rights. Therefore we must be thankful for any effort, from wherever it comes. And fundamentally it must come from the European Parliament. A joint effort, whether it is a matter of intercepting telephone communications, or the Internet, prepayment cards, whatever, also including money laundering, crimes against the interests and funds of the European Union itself, or crimes of terrorism, why not, but always with a counterweight of respect for fundamental rights.

And it never has been so. Now we are enjoying exactly this phenomenon, which benefits the person and allows a joint battle against organized crime. But we do not have to revert to the 19th century. It would be sufficient for us to return to the year 1950 in order to speak fundamentally of precedents regarding police cooperation and judicial cooperation. As a practical matter they began with the

European extradition treaty of 1957 and a European treaty on judicial assistance. And note that, if we examine the degree of voluntarism pursuant to which we joined together to defend ourselves against criminality, we can establish a series of phases, fundamentally three. A resistance phase, in which cooperation was a bit held back, related to cooperation in judicial assistance, the agreement implementing the Schengen treaty, and the judicial assistance treaty regarding criminal matters. Then, after these relationships consisting of extending a helping hand but at the same time withdrawing it, almost as if we were going to lose a finger in the interchange, because the mentality of people, even if delayed, understands that a common fight may be beneficial, may accomplish more than an individual fight, may reach further and be much more effective, we progressed to a sort of phase of cooperation and integration. At this point there is a series of legal instruments, also very important judicial instruments. It is the phase of liaison magistrates, that is, persons sent by one country to another country so that, in the country that is to receive a judicial order issued in the other, they are there as representatives, as agents, to carry the papers as quickly as possible from one office to another, in such manner that the judicial proceedings are expedited and take as little time as possible. This is the phase of the European judicial network, also the phase of Eurojust. Eurojust, like Europol, one for the police and the other for the courts, is a system that is invented, I am speaking literally, is truly invented by good thinkers, by lucid persons, intended to resolve the problem of judicial cooperation by greater integration. Fortunately, at least if we view it from this country, the greater integration of countries comes from what today is called the European Union.

And one need not be a mind reader to predict that from cooperation in integration it will become a matter of almost total integration. Here is the example of the European constitution with an institution that could be the European prosecutor's office, the only such office for the whole of Europe, or a prosecuting office for all of Europe, and also integration of the procedural laws of all countries so that they contain the least discrepancies in their content, making possible or facilitating more logical application, more natural than that of the existing legislations regarding procedural matters. These, as is logical regarding the subject matter we are discussing, are addressed to detention and capture of criminals to be tried, or detention and capture of criminals already convicted, above all and fundamentally so that they serve the sentences that courts, fully respecting the fundamental rights of those criminals, decided, in criminal trials, that they deserved.

This is the outlook. And we would say this is the current outlook. And surely it is a pretty outlook, a beautiful outlook. What is occurring is what typically also

occurs in the course of such disgraceful events, 11-S in New York, 11-M in Madrid, the events in London. There are those who, I admit, in an excess of zeal for punishment of conduct that obviously, I insist and I emphasize, is criminal in capital letters, feel an obligation to protect us in a manner that restricts our fundamental rights more than is necessary. And it is to avoid these, shall we say, possible or presumed abuses of power that may occur at a given time that the provisions of the European Union regarding judicial cooperation and police cooperation arise, as do the supervisory authorities that try to oversee what is happening with our treatment of personal data used to combat such execrable purposes as these forms of organized crime. And just as there are persons who, within the proportionality of what it is they are trying to combat, ask only and exclusively for what is necessary to effectively engage in that battle, and only for the time necessary in order for it to be ineffective, others have a tendency to unnecessarily invade our privacy. It must be remembered that this is a fundamental right contained in article 18 of the Constitution and, as regards protection of personal and computerized data, if I remember correctly, in section 4.

This is the approach, and this is what we have to deal with. And then there is the Schengen control authority, and Europol, the police authority, with its systems and files. Then there is Eurojust, the European arrest warrant, an instrument extremely effective in the battle, but always within respect for rights, minimum respect, the necessary respect for fundamental rights of an individual nature. I always remember the first judgment of the Spanish Constitutional Court, from the year 1993. I believe the Agency had not even been created. A citizen of Guipúzcoa sought to see the information about him in a given police file. In those times, which were already democratic times, obviously, he ultimately obtained from the Constitutional Court, when the first Data Protection Agency had not even been formed, nor was the first organic law, from 5/92, in effect, that declaration that every Spanish citizen has the right to know the information about him held in police files, and has the right of access, and has the right of rectification, and has the right, if applicable, of erasure.

We cannot lose our democratic path, which we must adopt, and limit our fundamental rights to the minimum extent necessary. And this has much to do with the supervisory authorities for each of the systems that maintain databases, be they police or judicial. An example of what I would not like to have happen is for us to have our own legislation. If you are interested in examining the former organic data protection law, Act 5/92, and have the current data protection statute, Act 15/99 of 13 December 1999, you will see that organic law 5/92 established jurisdiction over files related to the antiterrorist fight, that is with the limitations

that at that time for police files were contained in our legislation, which in principle and in fact were a result of a resolution issued at the appropriate time by the Council of Europe in application of agreement 108 regarding police data. But, as if by magic, in the current law terrorism files are excluded from the scope of protection of the personal data protection law. I believe this is a bad way to legislate. They should not be excluded, because there is no control, except the control of saying listen I have some files. Nobody controls the content of the files, for how long it is retained, which data are inaccurate. It deprives citizens of exercise of the rights of access, rectification, erasure, etc., etc. established in our law.

I would not like to reach that result on the pretext of combating terrorism. I believe that as persons, as nationals of European countries, we have a tradition, an experience and sufficient authority to combat the phenomenon of terrorism, while affecting our personal privacy to the minimum extent possible.

19

Why a European Judicial Area? Why Data Protection within this Area?

Fernando Irurzun[1]
Connsellor on Judicial Affairs in the Permanent Representation of Spain to the European Union

Building a European Area of Freedom, Security and Justice for many is one more step in the most ambitious project pursued by the political unit of democratic Europe: the "European Judicial Space is the richest area for progress regarding some key and universal questions in the European structure: the role of legislative harmonization as compared to mutual recognition, the role of community institutions as compared to national institutions, the political energy necessary to emerge from the mire of complexity" (Elizabeth Guigou).[2]

Without detracting from its political value, the European Judicial Area is, at the same time, a need that becomes more pressing every day. It is a necessary consequence of the elimination over the last 50 years of the barriers to free movement of persons, services, merchandise and capital among the Member States of the European Union. Greater integration of the national judicial systems in my judgment is the most effective response to the concerns of European citizens

[1] State Attorney and holder of a doctorate in Law. The opinions expressed herein are personal and reflect only the views of the author.

[2] Conference held in Brussels on 11 January 1999 by Cabinet Minister Jospin, with the title "Vers une Justice Européenne?"

regarding protection of their fundamental liberties, their aspirations for justice and security.

The effect of elimination of legal barriers and physical boundaries among the states of the European Union is seen in many neighbourhoods, not only in the capitals, but also cities and towns. For example, the number of citizens of other states in the European Union who take their vacations in a country other than their home country, have a second home there or even have permanently relocated is not inconsiderable. In some cases this results from the search for professional opportunities. In others the search is for living conditions more to their liking. And what can be said about the business and corporate world?!

The concerns of citizens also do not vary significantly from one side or the other of the former borders. Together with unemployment and economic status, crime, immigration and terrorism invariably appear in the first places on their lists of concerns, although they vary in degree of importance depending on the country or the time.[3]

Faced by this reality, we have judicial systems that are basically national, still in an incipient phase of integration. Although successes and improvements occur on a daily basis, there are still some hindrances owing to purely local or sovereign philosophies. The European tools within this Area, which have so much to do with the extensive criminal phenomena of our era (terrorism, organized crime and other serious crimes) have barely begun to be applied.

The existence of crimes with a European dimension

Reality of the European dimension that I invoke as a justification for a Justice Area, which is evident in some examples drawn from Spanish court records which, in turn, serve to illustrate the not inconsiderable amount that has been done and the many things that remain to be done.

We have been accustomed to confront the terrorism problem using an essentially national and bilateral focus (between two states or the neighbouring states). We must remember the efforts that the Spanish democratic institutions have made for years to understand the importance of transnational aspects in the fight against all kinds of terrorism. Over time, unfortunately other terrorist acts have occurred that in the manner of their perpetration transcend bilateral or regional geographical limits.

---

[3] See Eurobarometer 64.

A good example of the European dimension is the *Darkazanli* matter, illustrating the threats, successes and deficiencies of the fight against terrorism. A German citizen of Syrian extraction, accused by Spanish authorities of participation in the European network of Al-Qaeda, engaged in his allegedly terrorist activities from Germany. But the ramifications, in the form of trips, bank transactions and related judicial proceedings extended to Spain, Belgium and the United Kingdom.

Based on these facts Spanish courts sent various rogatory letters to Germany, and a European arrest warrant for surrender of Mr. Darkazanli to Spain. The specific result, as many know, was rejection of the surrender as a result of declaration of unconstitutionality[4] of the German law implementing the Framework Decision as it related to the European arrest warrant and surrender procedures between the Member States of the European Union,[5] the impossibility of claiming extradition because Germany does not extradite its own nationals and, at least at that time, the facts alleged were not criminal in Germany, by reason of the time they were committed.

Beyond the easy conclusion of a prophet of doom, and although there clearly are reasons for being dissatisfied by the lack of judicial response in the specific case, cooler analysis allows extraction of some positive consequences, if not regarding the specific case, then regarding the action undertaken by the European Union over recent years.

Thus, it must be acknowledged that it was necessary to eliminate the barriers to extradition or surrender of nationals and the European Arrest Warrant has done so. Indeed, although it would have been the one unwilling to perform its obligations, the degree of integration already achieved in the Union allows appeal to the Court of Justice of the European Communities using the procedure for non-compliance contemplated in article 35.7 of the Treaty of the European Union.

That the alleged facts could not be criminally prosecuted in Germany because the antiterrorist legislation allowing prosecution of such acts came after their commission, and as a direct result of incorporation into German law of the

---

[4] The judgment of the German Constitutional Court has been discussed by Eduardo Demetrio Crespo, "El caso Darkazanli…," *Diario La Ley nº 6441 of 15 March 2006,* and by Antonio Cuerda Riezu: "Comentario a la sentencia del Tribunal Constitucional Alemán de 18 de julio de 2005 que declara inconstitucional la ley alemana sobre la orden europea de detención y entrega." *Revista Europea de Derechos Fundamentales,* nº 6/2nd semester 2005.

[5] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

Framework Decision on combating terrorism, would confirm that it also was wise to establish a common definition of terrorism in the European Union.[6]

The second example relates to a different kind of criminality. Not terrorism or organized crime. Rather other serious kinds of crime the effects and possibilities of prosecution of which in a Area without border controls also require a European perspective.

I refer to the "King" case. A British citizen, condemned to 10 years in jail in the United Kingdom for strangling five women in order to abuse them, having served his sentence obtains a change of identity in order to facilitate reintegration and decides to start a new life in Spain. Here, as has been judicially determined, he commits two sex-related murders, in 1999 and 2003. In the meantime, an innocent person is preventively detained for 17 months. A DNA sample from a cigarette butt found near the body of the first young murder victim served as the basis for solving the crime, after he was suspected of the second crime.

I am not here interested in the ups and downs of police action in a southern county of England through INTERPOL to determine the domicile of Mr. King through the Spanish police.[7] The relevant question is whether we can continue to deal with these kinds of criminal problems involving, for example, "changes of identity," on a purely national basis or based on DNA samples taken strictly on a national basis, when we are dealing with situations where, with a passport and 100 euros one may travel in two hours from any point in England to the Spanish coast, protected by the anonymity provided by millions of tourists or temporary residents. Allow me to remind you that we are dealing with an attempt to avoid the murder of a second youth and months-long deprivation of liberty of an innocent person.

In my judgment, these and many other cases demonstrate that, wholly apart from the European fondness for the European Judicial Area project, there is no lack of arguments in favour of a European response based on the most absolute pragmatism.

I want to make it very clear that, when I speak of a European dimension of our judicial systems I am not proposing the disappearance of national jurisdiction or total harmonization of our legislations. Such measures not only would be unjustified or disproportionate but, in addition, would not necessarily be the most effective.

---

[6] Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism.

[7] In this regard see Diario de Sesiones del Congreso de los Diputados, no. 832, year 2003, pages 26129 and following.

Nor in our European context would mere classical cooperation formulas dressed up with improvements in their functioning (the frequent reliance on *good practices*) be sufficient. Something else is missing. It is the institutional or quasi-constitutional component that is at the root of the idea of the Justice Area, as included in the treaties since the Treaty of Amsterdam. As has been indicated in commentaries (see De Kerchove[8] and A. Nieto)[9] it has real meaning and must be implemented, as I will note later regarding protection of personal data.

In addition, the response must be consistent with the basic fundamentals of the European system, with our model of society, in order not to betray the essence of the European Being, as a contribution to a disturbed world seeking alternatives. Among these basic foundations there is no doubt that a preferential place is occupied by fundamental rights, as explicitly recognized in article 6 of the Treaty of the European Union and repeatedly emphasized by the Court of Justice.

The European responses to terrorism

As European institutions have indicated on many occasions,[10] terrorism attacks the values upon which the Union is based, and a terrorist act against a country affects the international community as a whole. The European response to terrorism arose with special intensity after the attacks of 11 September and continues to develop. I will limit myself to a quick note, by way of balance, concentrating on the European Judicial Space and related matters. First, through the common definition of the crime of terrorism, which was approved by the already cited Frame-

[8] "In the same way that an individual is at the same time a national of his State and a citizen of the Union (which gives him specific rights), the exercise by the Member States of their criminal jurisdiction is not confined only to the limits of their territories, but rather is exercised on a shared basis with the other Member States in the Space of the Union," De Kerchove, G. "La reconnaissance mutuelle des décisions pré-sentencielles en général ", in G. De Kerchove and A. Weyembergh (editors), *La reconnaissance mutuelle des décisions judiciaires pénales dans l'Union européenne,* Brussels, éd. de l'Université de Bruxelles, 2001, page 114.

[9] By contrast with "other areas of international criminal cooperation," the European Judicial Area is characterized "by a gradual overcoming of the most classic and important principle of international criminal law: that of *territoriality* and *state sovereignty*," Nieto A., "Fundamentos Constitucionales del Sistema Europeo de Derecho Penal," *Estudios de Derecho Judicial*, nº 61, 2004, pages 23 and following.

[10] By way of example, the Recommendation of the European Parliament addressed to the European Council and the Council regarding the Action Plan of the European Union countering terrorism, approved on 31 May 2005 (P6_TA (2005) 0219) and the Declaration on combating terrorism adopted by the European Council at its meeting of 25 March 2004.

work Decision of 13 June 2002. A document that requires all Member States to criminalize terrorism, with a long list of conduct related thereto. It is worth repeating that, until that time, only a minority of the Member States expressly covered the crime of terrorism in their criminal codes.

Together with this definition, an essential point in the action of the European Union, the Member States have been developing a more modern set of judicial cooperation instruments that, although their scope of application is not restricted to terrorism because they are of general application, are particularly suitable tools in combating this kind of crime. This is a set of rules inspired by the principle of mutual recognition of judicial decisions that applies to the freezing of property and evidence[11] and financial penalties[12] and soon will be complemented by provisions regarding recognition of the penalty of confiscation[13] and a European Evidence Warrant.[14]

From an organizational or institutional perspective, it is sufficient to recall that over recent years the capacities of Europol in combating terrorism have been strengthened, as an element of support for the capacities of national police forces. A new agency, Eurojust, has been created as a unit to coordinate and foster judicial cooperation against serious crimes, including terrorism.[15] Rules have been created by means of which it is possible to form joint investigation teams among the police, judges and prosecutors of the Member States.[16] Such teams already have been formed for specific cases of terrorism.

In this context it seems particularly relevant to me to refer to the many provisions that have been approved or are being studied on improvement of sources of information in combating terrorism. With no effort to be exhaustive, this is the case of the Decision on application of specific measures of police and judicial

---

[11] Council Framework Decision 2003/577/JHA of 22 July 2003, regarding the freezing of property and evidence.

[12] Framework Decision 2005/214/JHA of 24 February 2005, on the application of the principle of mutual recognition to financial penalties.

[13] Text agreed upon on a political basis, pending formal approval, that on a certain basis is complementary to Framework Decision 2005/212/JHA of 24 February 2005 on confiscation of crime-related proceeds, instrumentalities and property, which contains specific provisions regarding the penalty of confiscation for certain serious crimes, including terrorism.

[14] The Commission proposal was published in the Official Journal of the UE of …, but the negotiated text includes substantial amendments.

[15] Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime.

[16] Convention on Mutual Assistance in Criminal Matters among the Member States of the European Union of 29 May 2000 and (article 13) and Council Framework Decision 2002/463/JHA of 13 June 2002 on joint investigation teams.

cooperation in combating terrorism,[17] replaced by the most recent Decision on exchange of information and cooperation regarding crimes of terrorism;[18] of the Decision on new functions of the Schengen Information System;[19] and (in a more incipient phase of the legislative process) of the communication of the Comission on improved effectiveness, enhanced interoperability and synergy among the European databases in the Area of Justice and Internal Affairs.[20]

The measures adopted by the European Union are not strictly limited to judicial or police cooperation. In many other areas of action by European institutions rules have been adopted for purposes of prevention or mitigation. I will refer only to amendment of the community provisions regarding money laundering, through the Third directive, to adapt it to the need to prevent and combat terrorist financing[21] and, more recently, the directive on retention of telecommunications data.[22]

A more European view of the investigation and prosecution of the crime: specifically, the principle of availability

Combating terrorism is not the only objective of the European Judicial Area. It must be recalled that the objective contemplated in the Treaty of the European Union for the Area of Freedom, Security and Justice is "offering citizens a high degree of security." Other forms of highly topical criminality, as is the case with the treatment of human beings, deserve special attention on behalf of the dignity and freedom of men and women.

Given the limited scope contemplated in the Treaties regarding approximation of the legislations as regards definition of crimes and imposition of common penalties, when dealing with improving cooperation among judicial and police

---

[17] Council Decision 2003/48/JHA of 19 December 2002 on the implementation of specific measures for police and judicial cooperation to combat terrorism in accordance with article 4 of Common Position 2001/931/CFSP.

[18] Decision 2005/671/JHA of 20 September 2005.

[19] Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism.

[20] COM (2005) 597 final.

[21] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[22] Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

authorities the Treaty does not establish restrictions based on the seriousness or geographical effect of the crime:

— "the operational cooperation between the competent authorities, including the police ... in relation to prevention, detection and investigation of criminal affences" (article 30.1.a) TEU [Treaty of the European Union]), or
— "facilitating and accelerating cooperation between competent ministries and juditial or equivalent authorities ... in relation to proceedings and enforcement of decisions" (article 31.a) TEU).

The "King" case clearly illustrates that when we are dealing with prosecution of a crime committed in a member state it is increasingly difficult to adopt an exclusively national point of view. The "transnational" element may appear at any time.

It is not surprising that confronted by this situation the Member States have begun, albeit on a more or less timid basis, to implement global mechanisms or tools to confront the phenomenon. A notable example is offered by what has come to be called the principal of availability of information.

The conclusions of the European Council of 5 October 2004 included approval of the so-called "Hague Program." It was to renew the commitments made five years before in Tampere by the Heads of State and Government of the European Union.

Among the innovations included in this Program is the principal of availability of information. It means "that, throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State." This access to and availability of information is, nonetheless, subject to specific limits, notably those deriving from the principal of legality and respect for data protection.

Over recent months the Council has begun work to implement this principle and, simultaneously, the Commission has proposed a Framework Decision on the exchange of information under the principal of availability[23]. This work, curiously, has been overcome by the effort dedicated by the Council to a Swedish proposal regarding easing exchange of police information, the focus of which is not

[23] COM/2005/0490 final.

the same as that underlying the principal of availability. We will have to wait to see whether it stalls development of the latter.[24]

The philosophy underlying the principal of availability starts from treating the territory of the European Union as a single Space, with the constitutional consequences noted before. An Area in which, therefore, there should be no barriers preventing information relevant to the prosecution of a crime committed in the any part of this Area that is held by the competent authorities of a member state from being available to the equivalent authorities in the state prosecuting that crime.

There is much work to be done to implement this availability principal by way of regulation. Many matters remain to be defined. These include how the information will be made available (direct access, access to a system of indexes, indirect access), the concept of equivalent authority, the relationship between the information available for investigation and its use as evidence, the need for common rules regarding obtaining certain information (for example DNA), and the role of the police in obtaining the information.

The political commitment expressed in the Hague Program to implement the principal of availability of information was inextricably tied to the Union's capability of filling a void, the absence of common minimum standards regarding the protection of personal data processed in the context of police and judicial cooperation regarding criminal matters. This is a matter that of course already appeared in the Treaty of the European Union in connection with police cooperation. Its article 30.1.b) refers to the exchange of pertinent information "subject to the appropiate provisions on the protection of personal data." Thus the Commission has taken the position that, at the same time as approval of the proposal regarding the principal of availability, it would present a proposed Framework Decision on this other matter.[25]

---

[24] I refer to the proposed Framework Decision on simplification of exchange of information and intelligence among security forces of the Member States of the European Union, in particular as regards serious crimes, including acts of terrorism. With the same objective (but outside the institutional framework of the Treaties) Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria have signed a Treaty "regarding strengthening cross-border cooperation, in particular as regards combating terrorism, transborder crime and illegal immigration," signed in the German city of Prüm on 27 May 2005.

[25] COM (2005) 475 final. The European Data Protection Supervisor has issued an opinion regarding this initiative, which may be consulted on its website.

The necessary guarantees of fundamental rights: specifically, protection of personal data

One of the premises of the European Judicial Area has long been the need to respect fundamental rights. Among them, it is particularly relevant for me here to address the protection of personal data.

To date the European Union has no common legislation on data protection generally applicable within the scope of police and criminal judicial cooperation. There is nothing more than the special rules included in certain sector regulations,[26] the general framework of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, done at Strasbourg on 28 January 1981, and Recommendation number 87 of the Committee of Ministers of that Council on use of personal data in the law enforcement sector. Without discounting the importance of the Convention, above all because of its pioneer nature, it is appropriate to recall that its article 9 allows the establishment of specific exceptions, to the extent that they are contemplated by law and are a necessary measure in a democratic society for protection of security of the State, public security or repression of criminal violations. Any such authorization, lacking the most minimum approximation, is an open door to regulatory diversity among the Member States.

This is a differentiating characteristic (not exactly positive) of the Area of Freedom, Security and Justice by comparison with the Internal Market (the other large space in the European construction). When implementing the latter it was deemed to be essential to establish minimum common rules protecting the rights of individuals, at the same time allowing full development of the Internal Market through free movement of personal data (Directive 95/46/EEC).[27]

Intended to fill this gap is the proposed Framework Decision of the Council on protection of personal data processed in the context of police and judicial cooperation regarding criminal matters, presented by the Commission. Discussion of it has already begun within the European Parliament and the Council. I will ad-

---

[26] Convention of 26 July 1995 creating a European Police Office (the Europol Convention); the Convention of 25 June 1991 on Application of the Schengen Agreement; the already cited Decision creating Eurojust; and article 23 of the aforesaid Criminal Judicial Assistance Agreement of 2000.

[27] At another time I have referred to this parallelism and the successive attempts to provide the Third Pillar with data protection rules, and to certain general questions regarding the data protection system applicable in this area. I remit to that work: "Renforcer la confiance mutuelle: principe parlementaire et sécurité juridique" in the work edited by De Kerchove, G. and Weyembergh, A., *La confiance mutuelle dans l'espace pénale européen*. Éditions de l' Université de Bruxelles, Brussels, 2005.

dress it next, but not before a more general reflection on appropriate adaptation of this system of guarantees to the public interests that are relevant in police and judicial activities.

Judicial and police activities of course must include a system of safeguards regarding protection of personal data. The risks to personal privacy that may result from such activities are not few. But to me it also seems essential to make these guarantees compatible with effective action of the justice system managed by police and judicial authorities, since such action is addressed to protection of freedom and security of persons and defence of our democratic societies. We must try to get the balance between each of the elements of this specific system right. But I would note that the principle of proportionality requires the specificity of the system, by reason of the public rights and interests in play.

In addition, this is something common to all fundamental rights (and the protection of personal data should not be an exception). Legal professionals are accustomed to it, whether by reason of the difficult task of imparting justice and applying the law, or by reason of academic considerations.

The Spanish Constitutional Court so states in its Judgment 292/2000:

> The data protection right is not unlimited. Although the Constitution does not expressly impose specific limits on it, or defer to the Public Authorities for its definition, as it does regarding other fundamental rights, there is no doubt that it is among the constitutionally protected fundamental rights and legal interests, because that is required by the principle of unity of the Constitution (SSTC [Constitutional Court Judgments] 11/1981 of 8 April 1981, F.J. 7; 196/1987 of 11 December 1987, F.J. 6; and regarding art. 18, STC [Constitutional Court Judgment] 110/1984, F.J. 5). These limits may be either direct restrictions on the fundamental right itself, as alluded to before, or may be restrictions on the manner, time or place of exercise of the fundamental right. In the first case, regulating the limits is a manner of implementing the fundamental right. In the second case, the limits that are established are on the specific manner in which it is appropriate to exercise the authority comprising the content of the fundamental right in question. It is a way of regulating exercise, which may be established by the ordinary legislator under the provisions of art. 53.1 of the Constitution. (Legal basis 11).

In a manner even more specific and relevant for our purposes, the same judgment echoes other prior judgments and the case law of the European Human

Rights Tribunal, justifying the limitation or restriction of this fundamental right for reasons related to the prosecution of crimes:

> On many occasions this Court has stated that the prosecution and punishment of crime also is a proper element of constitutional protection, through which others are protected, such as the peace and security of the citizenry. These rights are also recognized in arts. 10.1 and 104.1 of the Constitution (more recent ones include SSTC 166/1999 of 27 September 1999, F.J. 2, and 127/2000 of 16 May 2000, F.J. 3.a; ATC [Supreme Court Decision] 155/1999 of 14 June 1999). The 1981 European Convention also deals with these requirements in its art. 9. As does the European Human Rights Tribunal, which when referring to the guarantee of individual and family privacy under art. 8 of the Human Rights Convention, also applicable to movements of personal data, recognizing that there may be limits such as security of the State (STEDH [European Human Rights Tribunal Judgment] in the Leander case of 26 March 1987, 47 and following), or prosecution of criminal violations (mutatis mutandis, SSTEDH [European Human Rights Tribunal Judgments], Z case of 25 February 1997, and Funke case of 25 February 1993), has required that such limitations be legally contemplated and indispensable to a democratic society. This implies that the law establishing the limits must be accessible to the individual affected by it, that the consequences must be foreseeable in order for the limitations to be applied to him, and that the limits must be required by a social imperative and be appropriate and proportional to the objective to be achieved (Judgments of the European Human Rights Tribunal, X and Y case of 26 March 1985; Leander case of 26 March 1987; Gaskin case of 7 July 1989; mutatis mutandis, Funke case of 25 February 1993; Z case of 25 February 1997). (Legal basis 9).

In the European Union, the Court of Justice will have an opportunity to analyze this principle in the context of the challenge by the European Parliament of the legal instruments allowing border control authorities in the United States to access data of passengers arriving on European flights.[28] Currently we have the

[28] Consolidated Matters 317/04 and 318/04, Parliament vs Council and Commission. Now that this matter has been published we know the judgment of the Court of Justice, issued on 30 May 2006, which voids the challenged acts (the Decision on adaptation issued by the Commission and the International Agreement signed by the European Community and the United States), holding that article 95 of the Treaty of the European Community based on harmonization of rules for the internal market is not a valid legal basis for those acts. The judgment nonetheless does not address the sufficiency of the guarantees contemplated in the two acts from the point of view of data protection.

conclusions of the Attorney General that reiterate this principal and hold that combating terrorism and other forms of crimes is a lawful purpose justifying restriction of the right of data protection, provided that the legality and proportionality parameters are satisfied.

Going now to the proposal of the Commission, we see an effort of this Institution to stay as close as possible to the content and structure of the Directive of 1995, at the same time incorporating certain provisions peculiar to the police or judicial context, taken from the Convention on Application of the Schengen Agreement, from the EUROPOL Convention and from the Eurojust Decision or from the most recent Prüm Treaty.

Based on the content, it is a general and complete rule including the criteria for determining the lawfulness of data processing, the rules governing transfer of data by and among the authorities, their international transfer, the classical rights of the interested party, the obligations regarding confidentiality and security, the guarantees in terms of responsibility and judicial monitoring, and a system of independent supervision.

Along the lines of other recent fluctuations in the jurisdictional dispute between the European Commission and the Member States, the establishment of sanctioning measures is proposed to assure full application of the Framework Decision. A new feature is that[29] there are to be criminal sanctions in the most serious cases.

There are many questions suggested by the text, and many comments that should be made. Limiting myself strictly to the time I have been given, I will concentrate on four specific matters that to me seem to be most important. In some of them we should particularly sense the peculiarities of the protectable rights and interests that pulsate behind the activities to which the Framework Decision is to be applied:

1. *The meaning of "minimum rule"*

The purpose of the Framework Decision is to give the Union a minimum level of harmonization of the national legislations, and is open to the possibility that the Member States may maintain or establish even greater guarantees or safeguards. This "*upward*" flexibility, nevertheless, should not detract from achievement of the other objective of this exercise. That is, based on this minimum level of guarantees,

[29] I refer to the dispute regarding community jurisdiction to impose an obligation on the Member States to assure compliance with obligations contemplated by community law by establishing criminal sanctions. This was decided as regards ecological crimes in the Court of Justice judgment of 13 September 2005, in matter C-176/03.

national obstacles based on data protection may not be erected against transfer of information relevant to the battle against crime in the European Judicial Area.

This is an element that also underlies the 1995 Directive, although logically as regards the Internal Market. It would be good for it to be clearly recognized in the Framework Decision.

2. *The purpose for which the data are collected and thereafter processed*

One of the fundamental principles regarding data protection is that data are to be collected for a lawful and specific purpose, and not used in a manner incompatible with that purpose. When that principle is transferred into the police and judicial sphere it quickly becomes necessary to establish how it is to be interpreted. From a strict or orthodox point of view it would be maintained that the purpose of the processing in these cases is the specific crime or criminal investigation for which the data have been collected. From a less strict point of view the purpose would be held to be criminal investigation.

Either interpretation has undesirable consequences. In the one case, an extreme interpretation would result in the data collected in the context of a specific crime being removed from police or judicial use in later investigations related to other crimes. Returning to our "King case," any DNA samples collected regarding one of the murders, or those that may have existed in the United Kingdom, or information regarding the *modus operandi* of a convicted or suspicious person, could not be compared or analyzed by the investigators.

A conclusion of this kind clearly has a disproportionate result that appears not to be justified by a proper weighing of the different fundamental rights involved. But in addition, as a practical matter a wonderful theoretical exercise would ruin the proper functioning of our crime prosecution systems, in particular police investigation.

The more generic interpretation also does not lack risk and danger of abuse, for example in the sense of leading to difficulty in application of other data protection principles, such as the purging of data not necessary to the purpose for which they were collected.

In my view what we have is a false dilemma, for which the law provides sufficient solution mechanisms. Something has already been said in this regard by the European Data Protection Supervisor, in his Report on the proposed Framework Decision. By contrast with the position taken by the Commission, he proposed, with the appropriate guarantees, more flexible restrictions on later use of the information. More specifically, the European Supervisor proposes (paragraphs 62 and following of his Report) that later use of the information be authorized for

prevention, investigation or prosecution of crimes, or for protection of the fundamental rights and interests of a person.

There are other possible elements of or paths to a solution. What is important is that one as influential as the European Data Protection Supervisor acknowledges the need for an approach to this problem apart from simplistic or maximalist interpretations.

3. *Some consequences of the legal nature of the authorities and actions to which the Framework Decision will be applied*

The Commission has opted for a single regulation of police and judicial matters, without distinguishing on the basis of the type of authority or proceedings in which the information is collected and used. Apart from one's opinion of this approach (I note that the Counsel of Europe addressed its Recommendation no. 87 only to processing of data by the police), we must deal with the terms of the proposed Framework Decision. Nevertheless, we must not lose sight of the fact that the legal nature of certain actions has specific implications regarding the content of the regulation.

To begin with what appears to be most simple, it seems obvious that the inclusion of a system of supervision by independent authorities must be accomplished without diminishing protection of judicial independence and the full jurisdiction of criminal courts to hear criminal matters. It is a fundamental principle upon which the European Union is founded (article 6 of the Treaty of the Union). I do not believe there is any doubt. Another matter is how it is to be implemented in practice, within the specific context of this proposal. The Commission seems to be satisfied with article 30.9, as follows:

> The powers of the supervisory authority shall not affect the independence of the judiciary, and the decision adopted by this authority shall be without prejudice to the execution of the legitimate tasks of the judiciary in criminal proceedings.

The formula to me does not appear to be sufficient. Perhaps a better source of inspiration is in the Data Protection Regulations of the Community Institutions themselves.[30] Article 46 thereof expressly excludes the "Court of Justice of the European Communities, acting in its judicial capacity" from the inspection authority of the European Data Protection Supervisor.

---

[30] Regulation EC 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the community institutions and bodies and on the free movement of such data.

The text of the Proposal nonetheless contains other possible points of friction that should not be discounted, given the environment we find ourselves in. An example is article 9.6, related to the right of the person involved to ask that data the accuracy of which he challenges be marked. As construed this appears to recognize a dual control system (of the courts and of the supervision authority) regarding such challenges.

A second kind of comment, related to the jurisdictional or potentially jurisdictional elements of the activities to which the Framework Decision is to apply, to limit the scope of the regulation and the existence of a data protection system. From a legal point of view this instrument will facilitate movement of information among the competent authorities of the Member States. But in no way will it detract from the need to continue distinguishing between information for investigation purposes and information for judicial evidence. Nor will it detract from applicability of provisions regarding judicial assistance or cooperation.

In fact it is not too much to remind ourselves that the policies of a member State must, when the principles of availability and data protection are within an appropriate legal framework, allow access to information in another member State, with the confidence that in the process of its collection the second state will act in accordance with minimum data protection standards. But at least until future legislative approximation within the European Union, that does not prevent continuing application of the criteria for admissibility of evidence in the state having access to the information.

A second reminder relates to the need to specify the relationship between the article of the Framework Decision that governs the transfer of the information received from another Member State among the various competent authorities in a given state, and the provisions governing judicial assistance. A first reading of article 12 of the proposal reveals nothing, for example, as to whether the judicial availability of the data received from the other state by a police authority requires satisfaction of judicial assistance procedures, taking into account the fact that they sometimes include other kinds of requirements or guarantees that are not covered by the data protection rules.

4. *Some necessary elements for exercise of recognized rights*

To conclude, we note the propriety of maximizing the effort to reconcile the exercise of the rights of the interested party with the characteristics of criminal proceedings and police investigations.

The text presented by the Commission already contains enough elements addressed to this purpose. Perhaps it would not be inappropriate to explore other

manners of regulating exercise of the rights, beyond mere exceptions (to allow the controller to properly satisfy his obligations, in order not to interfere with pending investigations, etc.). Perhaps it would be worthwhile to consider other alternatives, such as the possibility of indirect exercise (through the supervision authorities) of certain rights.

Allow me to emphasize a last point regarding a concern particularly held by those who work or have worked in the courts, which I hope will not be misinterpreted. We must be capable of creating a system that, while protecting the rights of the citizen, does not impose an intolerable bureaucratic burden on our courts. The practical implementation of the right of justice without undue delay, which also is a fundamental right, requires great effort and many resources, and not new burdens.

20

Data Protection and the Fight against Terrorism and Organised Crime: Joint Supervisory Bodies in the European Union

Peter Michael
Data Protection Secretary, Secretariat General of the Council of the European Union

Facilitating free movement of persons in the European Union is one of the important objectives of the Treaty on the European Union. Lifting the border controls between the Member States is symbolic for achieving this objective: without any form of border control, citizens may travel in the Union.

Another objective of the Union and closely linked with the creation of an area without internal frontiers, is to ensure the safety and security of the citizens of the Member States by establishing an area of freedom, security and justice. It is not possible to create an area of free movement without appropriate measures and close cooperation safeguarding important interests such as the fight against crime and terrorism.

Presently, various measures and forms of cooperation are established. Some are focussed on harmonization of national laws and policies, some stimulate cooperation including the creation of EU information systems and organizations. It will be interesting to focus on this last category since it also involves the creation of joint supervisory bodies.

One of the measures flanking the abolition of checks at internal borders was the creation of the Schengen Information System. Basic functionality of this system is to provide those authorities responsible for checks at the borders of the

"Schengen area" and the rest of the world, with information on behalf of all Schengen States. This information is also available for police controls. The categories of information processed in this system range from refusing entry to the Schengen area to warrants for arrest and extradition.

The second information system facilitates the exchange of data for customs purposes, the Customs Information System. This system assists in preventing, investigation and prosecution serious contraventions of national laws and improves the effectiveness of cooperation and control procedures of the customs administrations of the Member States.

Furthermore, two organizations were set up to stimulate the cooperation between law enforcement authorities: Europol and Eurojust. These organizations have the improvement of police (Europol) and judicial (Eurojust) cooperation between Member States as objective. Both organizations process law enforcement data from all Member States.

These four initiatives have two things in common. First, they all include the processing of personal data on a central point. Data from all Schengen and EU Member States are distributed to those central points. The legal instruments establishing the information systems and Europol and Eurojust contain the necessary data protection rules. The second common aspect is the creation of joint supervisory bodies for each of these systems or organizations.

Joint supervisory bodies

At present there are four joint supervisory bodies: they monitor the data processing by Europol, Eurojust and the use of the Schengen and Customs Information System and advice on all aspects relating to those activities. These bodies are composed of representatives of the national data protection supervisors. The independent status of these bodies is guaranteed by the legal instruments establishing these bodies, their composition and the explicit provision that the members are not bound by instructions in the exercise of their duties and subject only to the law.

The importance of the work of these joint supervisory bodies in the area of data protection and security can be demonstrated by the following:

— Each of these bodies have monitored the implementation and application of European data protection rules in specific area's of the objective of the European Union. They acquired practical knowledge on the influence of

European rules in the daily practice of European cooperation and exchange of personal data. Especially their monitoring task of different forms of data processing in European systems or organizations provided these bodies with information, not only on the processing of these data on a European level, but also on the practical implications when implementing European cooperation instruments on national level.

— These joint supervisory bodies are a platform in which representatives of all EU Member States data protection authorities share the same experiences enabling them and the national data protection authorities to create a better understanding of data protection requirements in a European setting. All these experiences have helped to create a level of common understanding of these requirements. Since European cooperation may be regarded as a process of gradual harmonization of national law enforcement legislation and practice as well as the national data protection regulations, these experiences are of great value.

Data protection and the fight against terrorism and organised crime

As already stated, the joint supervisory bodies have built up a great experience with the practical implications and consequences of European Union's initiatives to improve the fight against terrorism and organised crime. Some main findings of these bodies are:

— The creation of joint information systems as the Schengen and Customs Information System forced to specify *when* and which categories of personal data may be processed for specifically defined purposes. *When* these data may be processed is often regulated by national laws. Since these are not harmonized or at least not in all the area's covered by these information systems, the use of these systems demonstrates some significant differences between Member States.

— The use of such central information systems creates a risk for function creep. Once the information is processed for specific purposes, the availability of that information leads to new ideas and proposals for the use of that information for other purposes. This process undermines one of the important data protection principles: the limitation of the use of the data to the purpose for which they were collected.

— Europol and Eurojust have different tasks and information systems. For example, Europol is obliged to provide the Member States with knowledge and information facilities. It is especially these information facilities that demonstrate that the concept of European cooperation is still not on the level as foreseen by the Member States when they established Europol. The exchange of data with Europol is not on the level one would expect. Although there are different explanations for this situation, one important factor is the difference in laws, cultures and traditions in Member States when dealing with serious crime and terrorism.
— Another important subject of the Europol Convention and respective Council Acts, are the data protection conditions relating to the transfer of personal data to third states. Although both the Europol Convention and national laws in the Member States apply the same principles, practice has shown that Europol cannot transfer data to a particular state if that state is deemed not to have an adequate level of data protection, but where there is nothing preventing Member States from doing so by means of a bilateral agreement.

When the House of Lords Select Committee on the European Union requested the four supervisory bodies in 2004 to submit evidence in its enquiry into EU counter-terrorism activities, these bodies combined their experiences and reacted with a joint opinion to the House of Lords.

In that opinion the four supervisory bodies stated that:

— The EU-wide processing of large quantities of personal data, with access for intelligence and law enforcement agencies, is a significant development in the fight against terrorism and serious crime.
— Different EU proposals anticipate the processing of personal data from different sources on an unprecedented scale (retention of communications data), and introduce a new trend involving the collection of information on individuals (and not only suspects) with a view to aiding the prevention, investigation, detection and prosecution of crimes and terrorism.
— Apart from an assessment of the necessity of the proposals, there is the question whether the current data protection arrangements continue to provide an adequate level of protection for the individual. This question covers different aspects of data protection.
— The most important is the impact the different proposals may have on individuals. The fight against terrorism and other serious forms of crime is

not an isolated activity of one or two law enforcement agencies; it involves a huge number of agencies throughout the European Union. Personal data are processed and analyzed with the latest technology and made available to other authorities whenever considered necessary.

The experience of the Europol Joint Supervisory Body in assessing the agreement between Europol and the United States of America demonstrates that limiting the number of law enforcement authorities allowed to process the exchanged data is difficult. In the United States some 1500 authorities on Federal, State and community level are involved in dealing with criminal offences including terrorism.

— The processing of personal data on the scale proposed (often involving the processing of information on those who are not suspected of any crime) requires adequate legal safeguards such as purpose restriction, with supervision to ensure that there is compliance with legal instruments.
— The 1981 Council of Europe Convention for the Protection of Individuals to Automatic Processing of Personal Data (Convention 108) is perhaps too general in its nature to provide for an adequate set of data protection provisions dealing with the new dimension in processing personal data as set out in the different EU initiatives. Furthermore, there are significant differences in the way this Convention has been implemented by Member States in national law.
— A more specific set of data protection rules for police and intelligence authorities should be developed to enhance the level of data protection. The Commission recently proposed a Council Framework Decision on data protection in the third pillar. This proposal provides for a tailor-made set of rules applicable to law enforcement activities including the transfer of data to third states and bodies.

The European Data Protection Authorities concluded in a similar way when adopting their Declaration and Position Paper on data protection and law enforcement in Krakow on 24-25 April.

As a general conclusion when discussing data protection and law enforcement, one could say that the level of security justice and freedom in the EU is dependant on the success of the cooperation between Member States. This success is (partly) dependant on the level of harmonization where law enforcement is concerned, the harmonization of data protection legislation in the law enforcement area, and the existence of joint supervisory bodies creating an extra dimension in data protection.

21

Data Retention: Perspective of the European Telecommunications Network Operators Association

Cristina Vela
Chairperson Working Party on Data Protection - European Telecommunications Network Operators Association (ETNO)

Introduction

I wish to thank the organizers of this First European Conference for the opportunity they have given us to discuss here in Madrid such important, diverse and complex topics regarding data protection, from very diverse points of view.

I would like to briefly describe what ETNO is. ETNO is the European Telecommunications Network Operators Association. I have the honour of chairing its data protection working party. ETNO is comprised of 41 telecommunications groups from 34 European countries. It was created here in Madrid in 1992. The ETNO members have around one million employees throughout Europe. The fundamental purpose of ETNO is to defend the common interests of its members as regards the activities of European institutions and other community agencies, and so contribute to development of policies promoting the Information Society in Europe.

Data Protection versus Data Retention

Before discussing the recently approved Data Retention Directive, I would like to address the Data Protection Directive for the electronic communications sector (Directive 200/58/EC), a sector directive that was a part of the so-called new regulatory framework for electronic communications approved in 2002. This directive, which implements the general principles of the Framework Directive of 1995, applied to the specific characteristics of the telecommunications sector, in its article 15 had already established the possibility that the Member States might introduce data retention obligations of general application. It was a possibility, not an obligation, but various Member States began to implement this provision. This for example was the case in Spain, where the e-commerce law established the possibility of a generalized data retention obligation for up to a maximum of 12 months. This obligation was established in the law, but was not thereafter implemented by regulation. Thus as a practical matter the data retention obligation was not in force. In other European countries, although rules also were adopted at the level of laws, thereafter there was no implementation at the regulatory level. Thus, as a practical matter there was no data retention obligation.

There was a possible exception to the substantial obligations regarding data protection imposed by Directive 2002/58/EC.

Nevertheless, as a result of the terrible attacks in Madrid in March 2004, the Summit of Heads of State and Governments on 25 March 2004 adopted its Declaration regarding the fight against terrorism. It established the need to adopt specific measures regarding security before June 2005. Among these security measures there was specific reference to measures regarding data retention for traffic in electronic communications.

Very quickly, scarcely a month afterwards, at a meeting of the Council of Ministers of Justice and Interior held on 28 April 2004, four Member States introduced a joint initiative, the so-called proposal of a Framework Decision regarding data retention. This was quite unexpected, because these four Member States only gave one day's notice to the European Commission that they were going to present this regulatory proposal. The four states that initiated this proposal were the United Kingdom, Ireland (which then occupied the presidency of the Union), France and Sweden. Throughout the entire process of adoption of the now directive regarding data retention these countries have been very active. Thereafter, with the attacks of July 2005, when Britain

occupied the Presidency of the Union, which began in that same month of July, the political will to adopt a data retention regulation was just strengthened.

Proposal of Framework Decision versus Proposal of Directive

Very briefly, the Proposal of a Framework Decision regarding data retention is a regulatory proposal that has for a long time run in parallel with the later Proposed Directive of the Commission. The objective of a Framework Decision is to harmonize existing legislations of the Member States (as we have said, it is clear that in some Member States there already were data retention regulations) and relates to policies under the so-called third pillar, justice and internal policies.

More than a year and a half after the initial proposal of the Council, the Commission adopted its Proposed Directive. Thus there were problems in deciding on the appropriate legal basis for adoption of data retention measures.

The Council and many Member States maintained that it was a matter covered by the third pillar and, therefore, the Council was competent, not only to propose it but also to adopt it unanimously, with only a non-binding opinion of the European Parliament.

On the other hand, the Commission itself and the European Parliament, as well as the Council's legal department, maintained that a directive was necessary, a directive harmonizing the internal market. Ultimately this was the legal basis that was used. The content of both proposals was very similar regarding types of data to retain and retention periods. It was basically an institutional discussion regarding the appropriate legal basis, regarding which agency was responsible for proposing regulations and finally adopting them.

As it ultimately was a directive, the European Parliament has had a significant role. It became the co-legislator, at the same level as the Council. The European Parliament here asserted the need for it to have a voice in adoption of regulations of this kind, not just a non-binding opinion.

As Rosa Díez commented before, the adoption of this directive was very rapid. The Proposal of the Commission was presented on 21 September 2005 and the Council adopted a resolution on 2 December. This resolution was ratified by the European Parliament in mid-December, with a vote at a plenary session in Strasbourg. The Commission immediately accepted the amendments, some substantial, that both the Council and the Parliament had introduced to its initial proposal, and so approved the resolution adopted by the Parliament and the

Council. Finally formal adoption by the Council occurred in February 2006, with only publication in the Official Journal remaining.[1] Some countries continued to question the propriety of the legal basis. These included Ireland, which continued to maintain that a framework decision of the Council was the appropriate legal act. But because in this case, as in the case of a directive, not unanimity but just a qualified majority is required, the directive was adopted.

Principal Topics in the Directive

I would like to highlight the principal points of the directive. We may consider it to be a directive of minimums. Therefore, it may be questioned whether this directive will really achieve the objective of harmonization, because many of the key aspects of its content depend on later adoption at the national level by the Member States. This may result in a risk to harmonization, which was exactly what justified a directive at the European level.

As Rosa Díez mentioned, the directive establishes a general obligation to retain traffic and localization data for electronic communications, to assure that this data is available for purposes of investigation, prevention, detection and prosecution of serious crimes.

The definition of "serious crimes" is one of the points remaining for later definition by the Member States, although it is true that reference has been made to the list of serious crimes appearing in the European Arrest Warrant, which may serve as a reference regarding which serious crimes may justify an application for access to retained data.

The *persons obligated* to retain the data are the providers of public networks for electronic communications and electronic communication service providers, with respect to the data of their customers, that is data related to the services provided by them.

The *data to be retained* are the data necessary to identify the origin and destination of the communication, the date, the time, the duration of the communication, the kind of communication, the terminal equipment from which the electronic communication is initiated and also the data regarding location in the case of mobile communications (art. 5 of the directive). The directive expressly excludes data regarding the content of the communications.

---

[1] The directive on data retention (Directive 2006/24/EC) was published in Official Journal L 105 of 13 April 2006.

Regarding *retention periods,* from the initial proposals of the Council, which spoke of two years up to even five years of retention, the retention period has been reduced. The Commission proposed a fixed retention period in all Member States for all kinds of data. Ultimately a compromise was reached, between 6 and 24 months for all kinds of data, whether fixed telephony, mobile telephony or the Internet. But as we said, it is a directive of minimums. The Member States may establish even periods in excess of 24 months in cases of special national situations justifying it. To do so, they must notify the Council.

From the point of view of the European industry we believe these terms of up to 24 months are excessive. The fact that data are retained for a greater term does not automatically result in greater effectiveness, because if they are retained for more time the necessary management systems are more complex and response time is lengthened.

There are other obligations affecting electronic communications operators and service providers, such as:

— assuring the quality and security of the retained data,
— the obligation to transfer the data requested by the competent authorities without delay (the directive does not define what is meant by "without delay").

Conditions and procedures for accessing the data also are outside the scope of the directive and await later definition by the Member States. The directive does state that the supervising authorities may be the national data protection authorities themselves.

The *compensation for the resulting costs* has been much discussed. Ultimately it was left outside the scope of the directive. The Commission in principle was more supportive than the Council of having a provision regarding compensation of costs, but ultimately it was not included in the directive. The Commission did note that a Member State's compensation of its operators for the costs arising from the retention obligation would not be considered to be an illegal state subsidy. Nevertheless, the fact that one member state decides to compensate the costs incurred and another does not may result in distortion of competition, affecting those to whom the directive is principally addressed, the telecommunications operators. The United Kingdom, for example, one of the countries that have led this legislative initiative, is very much in favour of the establishment of a system for compensation of costs. In fact, it has attempted to convince other European countries of the need for such a system. From the point of view of an association

that represents operators from very diverse countries, we believe that this is one of the points with respect to which the required harmonization will not occur. Therefore there may be a competitive disadvantage for operators.

Regarding *transition*, there are 18 months for adoption of the necessary national regulations. In addition there is the possibility that the Member States may opt for an additional 18 months extension to implement provisions regarding Internet traffic data.

This transition period will be necessary to discuss the technical implications that are arising and at the level of the directive ultimately have not been resolved. When implementing regulations at the national level it will be very important to actually define the most technical aspects in order for the national regulations to satisfy the objectives initially established.

The directive provides that its application must be evaluated three years after adoption. For that purpose the Commission will present a report to the Council and the European Parliament, a report based on statistics that the Member States themselves will provide regarding application of the directive.

The need to create a working party to evaluate the directive has been much discussed. The Commission has repeatedly stated the need for creating this group, comprised of not only representatives of the Member States but also of the European Parliament, the European Data Protection Supervisor and the industry. This also was a part of one of the schedules to the directive, which ultimately disappeared, and now is simply recognized in a whereas clause. On behalf of the industry, we believe this working party is key, because it will allow a discussion of important points regarding technological developments, the effect of application of this directive, not only in the industry but also in society (for example: loss of user confidence in use of electronic communications).

Therefore, within the European Network Operators Association we are already working to interchange information among the member operators regarding national developments in implementation of the directive. We are also working to assure creation of this working party proposed by the Commission. We believe it is key, immediately, to call on national data protection authorities, representatives of the article 29 Working Party, to emphasize the need for this working party (Whereas Clause 14) and ask the European Commission to organize a first working meeting as soon as possible, before the end of this year. On behalf of the industry, we believe it is necessary to assure appropriate representation of network and service operators, the principal subjects of the obligations established in this directive.

Experience of the Industry

The industry is totally committed to cooperation with the security forces of the state, and always has been. But experience shows us that the data requested by the security forces of the state in most cases is only three months old. This table is provided by the operator Telia Sonera, which does business in various Scandinavian countries. The figures are the same for the majority of operators.

For example, in the case of the Madrid attacks, when all of the Spanish operators made themselves immediately available to the judicial and police authorities, the data that were requested went back to December 2003, that is three to four months prior to the attacks. The data were already available, because the operators had the data because they were being stored for purposes of invoicing. Thus the industry asks itself: "Is it really necessary to have a data obligation that takes us up to 24 months, when the majority of requests for access to this data is for very recent data?" "Where is the principle of proportionality between such a broad data retention obligation and the real need for and usefulness of this data?"

Conclusions

In conclusion, we electronic communications operators find ourselves between very strict data protection standards and, on the other hand, now very broad data retention regulations. *On behalf of the European industry, we repeat, there is total commitment of electronic communications operators to cooperate with security forces of the state in prevention and investigation of serious crimes, particularly terrorism,* but we also would like to emphasize a point that was discussed just this afternoon, the importance of and *need for better police and judicial cooperation* allowing the shortening of very long proceedings. In this way the need to resort to historical data two, three, or four years old would be reduced. And this of course would result in greater efficiency in prosecution of crimes.

For the operators present in various Member States it is important that, when implementing the directive in the different Member States, any distorting effect on competition is avoided. Precisely because this is a harmonization directive, what should be attempted is harmonizing and avoiding different treatment in different Member States. *It is important to take this need for harmonization into account regarding matters such as retention periods, kinds of data to be retained and costs.*

Another important point is that *a very extensive data retention obligation could have a negative impact on the use of new electronic communications services*. We must avoid this loss of user confidence. Only a robust data protection system will increase consumer confidence in new services. Therefore we believe the data protection system already in place in the European Union and the various Member States is key to development of the information society in Europe.

By way of conclusion, at this conference we have repeated that data protection is a recognized Fundamental Right. Therefore, when adopting any national regulations on data retention in implementation of the European Directive it is very important to respect:

— the principle of proportionality (proportionality between the associated costs in economic terms and in social terms and the objectives to be achieved and benefits to be derived),
— effectiveness, that is that every regulatory measure on data retention is in fact useful in achieving the objective that has been established, which is to assist in the fight against organized crime and terrorism,
— technical practicability of any regulatory measure. Technical limitations must be taken into account.

On behalf of ETNO, as a representative of the European industry, we commit to continue cooperating in this environment of proportionality, adaptation and effectiveness of implementation of the directive, with the objective that regulations of this kind that may constitute an exception to fundamental rights be truly effective and well founded.

22

Data Retention

Francesco Pizzetti
President, Italian Data Protection Authority

Europe is the home of the concept that regulates the processing of personal data and their protection does not represent merely a set of rules to overcome intra-European barriers, but rather a veritable constituent of citizenship.

After Strasbourg Convention no. 108/1981, which first opened up the road towards affirming the right to self-determination in the use of personal data, the 1995 directive on personal data by the European Community set out binding, more homogeneous rules.

The directive was aimed at bringing about not only harmonised national levels of data protection to ensure full implementation of the single market, but actually at "maximising" data protection within the framework of the fundamental right to self-determination—which is not expressly mentioned, but is unquestionably recognised.

One might argue that the Europe of citizens and their rights started existing with privacy.

The legal and institutional rationale underlying this regulatory instrument, which was developed in a Community context quite different from the current one, was the forerunner of developments in the common area of freedom, security and justice that resulted in the new, more central role data protection has come to play over the past few years.

From this viewpoint, the directive was at the forefront of the evolution of Community institutions and of the Union towards a supranational political entity based on the fundamental rights shared by European peoples, and now recognised in the Charter of Fundamental Rights of the Union and in the Treaty establishing a Constitution for Europe.

Indeed, the implementation of all the tools and regulatory measures that allow the effective protection of personal data has become increasingly important in order to maintain the democratic character of our societies and to safeguard the dignity of European citizens.

This is why both the Italian data protection authority and the Article 29 Working Party have long been highlighting how important it is to ensure the effective, broad-ranging protection of this fundamental right also in sectors where this has been lower so far.

I think one can argue that the European focus has been shifting, during the past few years, from expansion of the four fundamental freedoms to an increased attention paid also to security issues.

Indeed, there are several signals pointing to this trend, including the recent adoption of the directive on retention of telephone and electronic communications traffic data, i.e. the so-called data retention directive.

On this point, our Authorities are bound to have something to say.

At European level, there had long been harmonised rules applying to the protection of data in electronic communications, which had been initially adopted in 1997 (directive 97/66/EC) and subsequently updated in 2002 (directive 2002/58/EC). They had introduced common principles to be complied with in processing telephone and electronic communications traffic data.

In principle, such traffic data related to subscribers, as processed by the provider of a public network or a publicly available electronic communications service, must be erased or made anonymous once they are no longer necessary for the purpose of transmitting a communication (pursuant to Article 6(1) of directive 2002/58, where the same wording is used as in Article 6(1) of the previous 97/66 directive). The only exception allows processing of data for the purpose of billing and interconnection payments up to the end of the period during which the bill may be lawfully challenged and payment pursued.

Indeed, as also related to this exception, the European data protection authorities considered (see their Opinion 1/2003) that there should be a harmonised interpretation of the retention period (3 to 6 months), by stressing that only adequate, relevant, and non-excessive data may be processed in respect of the aforementioned billing and payment purposes; all other data must be erased immediately.

However, directive 2002/58 allows Member States to only derogate from this rule where it is necessary to introduce a measure that is both necessary and proportionate, in a democratic society, to safeguard national security, enable prosecution of criminal offences, etc. Only on the above grounds, indeed, Member States could pass legislation setting out that the data may be retained in any case (irrespective of the existence of billing or interconnection payment requirements, as is the case with free Internet access) or else for an additional period (once the said requirements have ceased to apply). Still, this may only be done for a limited time span.

Concerning these provisions, the European Article 29 Working Party has repeatedly drawn attention to the need for stringently complying with the preconditions set out in the directive in order to derogate from the general rule.

In so doing, the Working Party has followed and strengthened the general principles of the right of privacy.

Indeed, the Working Party, also pursuant to the case law of the European Court of Human Rights, has always stated clear that any interference with the right to privacy may only be allowed for if there is an appropriate legal basis; if the said interference is necessary in a democratic society; if it is compliant with one of the lawful obligations mentioned in the European Human Rights Convention.

The blanket collection of traffic data impacts on a founding principle of the rule of law in contemporary society. The new right to personal data protection, being a fundamental component in order to fully recognise human dignity, entails the need to consider the proportionality of any measure limiting it, as well as requiring publicity and disclosure of the relevant rules. Citizens must be informed of the circumstances under which States and public authorities may develop intrusive surveillance mechanisms in respect of their conduct, in particular on their possibility to exercise fundamental freedoms such as the right to communicate.

Additionally, they must be in a position to be aware and evaluate the attending risks, both in order to adjust their behaviour, so as to prevent unwanted intrusions, and to gauge the right balance between security and freedom requirements.

Especially in the wake of the 9/11 attacks, there has been a pressing demand for new legislation enabling police and judicial authorities to avail themselves of the informational opportunities brought about by new technologies, in order to achieve an increasingly widespread, preventive and invasive control of—in particular—electronic communications. This trend was compounded further after the attacks in Madrid and London.

This led to the introduction of new provisions in some countries, as was the case in Italy in summer 2005.

On 25 March 2004 European Council Declaration on combating terrorism asked for the adoption of an instrument on retention of communication data by service providers, until June 2005.

In this panorama, in April 2004, four EU countries (France, Ireland, United Kingdom, and Sweden) presented a proposal for the adoption of a framework decision on the retention of telephone and electronic communications traffic data for law enforcement purposes.

Referring to this proposal, the Article 29 Working Party, in its Opinion no. 9/2004, firmly reiterated principles that had already been recalled on the occasion of the Spring Conferences of European data protection authorities held in Stockholm (May 2000) and Athens (May 2001), as well as being re-affirmed on other occasions—in particular, during the 2002 Cardiff international conference.

At the same time, the European Commission expressed some reservations on the legal basis applying to the proposal put forward by the four Member States mentioned above: in the Commission's view, any exceptions to directive 2002/58 were to fall, in any case, within the scope of application of "First Pillar" legislation and be grounded on Article 95 of the Treaty.

Thus, on 21 September 2005, the Commission submitted a draft directive on data retention, subject to the co-decision procedure involving the European Parliament.

About this draft directive, on 21 October 2005, the Article 29 Working Party issued an opinion, in which it recalled that the retention of traffic data impacts on the fundamental, inviolable right to confidentiality of communications. Consequently, any restrictions must be grounded on a demonstrable "pressing need" and, therefore, are allowed not because "helpful" or desirable in view of countering crime, but only in exceptional cases, for a limited period and in the presence of adequate safeguards.

Starting from this assumption and bearing these fundamental values in mind, the Working Party suggested some specific amendments to the draft directive. In particular: the retention period should be as short as possible and be regarded, in any case, as the maximum threshold applying to all Member States, which are nevertheless free to lay down shorter retention periods; the data must be erased at the expiry of the relevant period; the provisions in question must be time-limited (the Working Party considered three years as an appropriate term), and cease to take affect thereafter subject to a new decision by the Council and the Parliament (sunset clause requirement).

As for the purposes, the Working Party requested that the law enforcement bodies entitled to access the data should be specified, and that the data should only be accessed in connection with specific investigations. Additionally, it stated that data accesses should be logged; that the service providers concerned by the obligations in question should be specified; that providers should not be allowed to process the data they had stored for judicial and police purposes for whatever different purposes; and that the systems used for storing the data in connection with the aforesaid purposes should be logically separated from other systems and protected by means of enhanced security measures. In its Opinion, the Working Party also requested that the personal data to be retained should be specifically mentioned, whereby the contents of communications and traffic data related to "unsuccessful" calls were to be excluded and location data limited to the cell-ID at the outset of the communication. Finally, personal data protection authorities should be entrusted with supervising over lawfulness and fairness of processing operations in this sector.

I recalled the main points raised in the opinion by the Working Party to highlight the concrete approach that must be followed in order to defend fundamental rights of citizens as related to the protection of their personal data.

The European Parliament, initially, shared the considerations made by the European data protection authorities. Subsequently, on 15 December 2005, the same Parliament accepted—unfortunately—an agreement negotiated with the Council of the EU, mirroring the stance adopted by the Justice and Home Affairs Council on 1 December 2005.

This stance was remote from the requests made in the Opinion by the Working Party as for some especially important issues.

The points raised by the Council, which were agreed upon by both the Parliament and the Commission, envisaged a retention period ranging from 6 months to 2 years in respect of all data—including those related to "unsuccessful calls"; the obligation to retain the data related to Internet accesses, Internet e-mails and Internet telephony; the referral to domestic legislation in respect of the costs to be incurred by providers and operators.

Based on this framework, the Council finally adopted the directive at its meeting of 23 February 2006.

However, in this month (March 2006), the Article 29 Working Party had, once again, re-affirmed the need for national lawmakers to pay appropriate attention in order to ensure that the implementation of the obligations referred to above, goes hand in hand with measures reducing their impact on the rights of individuals.

We as Europeans cannot, must not, and do not want to accept that we should live in a society based on suspicion and control.

With its new position paper of March, the Working Party meant to underline the serious concerns shared by data protection authorities in the face of a trend that, if uncontrolled, might be remarkably prejudicial to our freedoms.

Implementing the data retention directive will result into storing billions of information data. This information concerns the lives of all European citizens, and it must be protected, safeguarded and used only by authorised entities for the purposes set out in the law.

Let me quote an Italian example. In Italy, this means 200 millions of conversations and 300 millions of mobile telephony "events" stored per single day. A monitoring initiative undertaken by the Italian Garante 3 years ago, which only considered the 5 biggest operators and did not take account of incoming calls and unsuccessful calls, calculated 700 billions of data to be stored annually as for telephone traffic only.

The data concerning Internet supplied by the Italian Internet Providers Association show that 2,400,000 gigabytes should be retained yearly as regards e-mails, without considering the log files related to all other electronic communications services.

We should all be aware that there is a problem related to ensuring security of such huge databases against possible intrusions; on this point, all the Authorities should be called upon to take effective action.

The data retention directive, the draft framework decision on the availability principle presented by the Commission on 12 October 2005, and the other instruments so far adopted, and furthermore under discussion (SIS-II e VIS) within the framework of judicial and police cooperation show that the circulation of personal data—in particular, those related to electronic communications—is bound to attain unprecedented qualitative and quantitative features.

The unrelenting increase in the number and type of the data stored in information systems entails increased risks for citizens' right to privacy.

We are facing something more than the well-known issue of how to reconcile privacy and fight against crime.

For the first time, in Europe, under the colour of law, there is an obligation for private entities such as service providers to retain, for police and judicial purposes, data that otherwise should not be collected or else should be erased expeditiously.

All these considerations raise a deep-ranging ethical issue we should be capable to address also in a cultural perspective, before data retention spreads out to

include other sectors such as Internet cafes, wi-fi services, GPS networks, interactive TV services, public facilities, transportation, private contracts, consumptions, etc.

We Europeans are running the risk of turning our democratic societies grounded on the respect for, and defence of, everybody's freedoms into oppressive surveillance societies. No European should accept to pay such a high price for the sake of security. No European should accept to sell one's own soul, grounded on Europe's legal tradition, for the sake of his or her body.

Bearing these concerns and huge risks in mind, one can understand why European data protection authorities have long urged the EU Institutions to extend full-fledged data protection safeguards to personal data within the framework of the so-called "Third Pillar" activities.

This was re-affirmed also during the latest Spring Conference at Krakow, in April 2005, and the Vice-President of the European Commission, Mr. Frattini, has taken note repeatedly of this stance.

This can explain why the Article 29 Working Party, in its Opinion on 24 January 2006, welcomed the presentation by the Commission (on 4 October 2005) of a draft framework decision on the protection of personal data in the Third Pillar.

The attention paid to the fair, lawful use of personal information at a time when, in both the EU and the international and national communities, values, interests and decisions aimed at enhancing citizens' security are becoming increasingly important is a fundamental signal we should give in order to defend our own cultural identity and traditions.

However, this is also a benchmark for the soundness of the legal framework related to privacy and its capability to adjust to the evolution of the contexts in which it is to be implemented.

In the data protection sector, it is increasingly important for regulation and defence of principles to be accompanied by enforcement and control in respect of compliance with such principles.

To protect the dignity of individuals and the democratic character of our societies, we, as data protection authorities, are called upon to play an increasingly effective, dynamic supervisory role concerning processing and concrete safeguards applying to the data in question. This requires national data protection authorities to be strong, provided with powers and functions that can impact on regulatory patterns, and fully capable to control lawfulness of processing operations in each Member State and in all the European Union.

This is the reason because the Article 29 Working Party, in its Opinion of 24 January 2006, has affirmed that the same Working Party, beside national DPAs

and the European Data Protection Supervisor, should come to play an increasingly effective role also in operational terms.

The first long, vibrant phase in the history of European privacy was marked by a mainly cultural, regulation-oriented approach. In order to ensure full recognition of the right to privacy, emphasis was put on its inherent connection with the protection of human dignity and the focus was mainly on setting out legal rules.

Now, is the time to start a new phase, featuring not only the broader expansion of such rules and their safeguards, but also the appropriate mix of regulation and enforcement.

The concrete, careful assessment of the manner and mechanisms whereby data are processed is increasingly necessary in order to ensure an acceptable balance between security and freedom.

None better than data protection authorities can carry out this task, and that is why we feel reassured by the importance attached to these authorities by the Charter of Fundamental Rights of the EU and the forthcoming European constitutional Treaty.

Terrorism and organised crime are neither new nor short-term phenomena. It is likely that we will have to live with them for a long time. The challenge we face in defending not only our society, but also our liberty, bears upon our freedom and spontaneity in communicating and expressing our opinions on the nets.

Therefore, our role is increasingly focusing on this fundamental goal: the search for the ever-advanced balance between individual and social rights and freedoms, on one hand, and, on the other hand, the defence of peaceful social coexistence. Our task is to ensure that this fundamental framework is concretely and effectively struck in all sectors of our lives.

We, as Europeans, cannot accept to consider data protection and the fight against crime as alternative values.

We will never accept that they should be played one against the other.

Part vi

DATA PROTECTION AND TRANSPARENCY: DEVELOPMENTS IN TELECOMMUNICATIONS AND PRIVACY

23

Data Protection and the New Information Technologies

Francisco Fonseca
Director of Civil Justice, Fundamental Rights and Citizenship, in the Directorate-General for Justice, Freedom and Security

For me it is a pleasure to take part in this First European Data Protection Conference. First I wish to congratulate the Director of the Agency, Mr. José Luis Piñar for the excellent initiative in holding this First European Data Protection Conference. I would also like to thank him for his invitation to attend and the timing: data protection is at a point where it is increasingly discussed, and there is general awareness of the importance of this fundamental right of the person to the progress of our society.

In the time that is given me I would like to share with you some reflections of Commission personnel regarding the relationship between data protection and the new information technologies. I will try to explain where we find ourselves, the challenges that new technologies present to personal data protection, for that purpose bearing in mind the work we are carrying out.

I will first address the main questions presented by existing regulations, in particular the fact that they may not be appropriately adapted to the requirements of the new information technologies. Then I will address the current work of Commission personnel regarding such matters as RFID, PETs and the Internet. As you will see, I am not going to identify final solutions for these matters, which are still under discussion. I will limit myself to sharing with you certain considerations

that, in the judgment of Commission personnel, should be a part of this discussion.

New Technologies versus Personal Data Protection …

It is often stated that data protection and the new information technologies are antithetical, pursuing different objectives and ends. For some data protection, to the extent that it requires considering a series of matters related to processing the personal data that is obtained, used or transferred, hinders or prevents development of information technologies, and that would interfere with technological progress and social development. And that progress is inevitable in a world characterized by growing use of these technologies. Attempting to respect principles of personal data protection is unrealistic. Doing so would require all of those developing new information systems and new programs to undertake very complex work to adapt them and limit the capacities of the systems. And ultimately not even that would guarantee that the systems developed would respect data protection principles. The new technologies are so complex that they make it impossible to adapt them to the requirements of data protection. In addition the European personal data protection regulations (Directive 95/46/EC) date from a time, 1995, when information technologies had not expanded as they now have. Therefore the 1995 Directive has not been able to absorb this phenomenon and cannot be an appropriate framework.

Faced by this reductionist position, it is necessary to remember that when we speak of personal data protection we are speaking of a fundamental right of the person. It has been so recognized by international documents, such as the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe. Article 8 thereof, regarding the right to privacy, has served as the basis for the Human Rights Tribunal of the Council of Europe to address matters related to personal data protection. It also has been recognized by community documents, such as the Charter of Fundamental Rights of the EU and Directive 95/46 on protection of personal data. Finally it has been recognized by the constitutions of the Member States.

If it is a fundamental right, the question presented is not whether the new information technologies can be developed *ad infinitum* apart from data protection. It is obvious that no one, in particular the authorities responsible for personal data protection, is opposed to the new technologies and their development. Nor do they deny the advantages they offer. Rather, the question is to determine how

and in what way the new information technologies must be developed and applied so that the essential content of the fundamental right to personal data protection and the right to privacy are at all times guaranteed and can be protected by the public authorities. Clearly we are faced by two distinct realities, located at two different levels, a fundamental right and an economic activity. And the latter must take the former into account if it truly wishes to present itself as respecting and being consistent with the fundamental rights of the person. It cannot be argued that these fundamental rights must yield or have their content limited in the event of use of information technologies that by their nature or design involve invasion of privacy.

The Article 29 Working Party has confirmed this position in several of its working documents and opinions adopted over recent years, specifically related to information technologies. I therefore would say that it is a matter of determining how to reconcile the two matters and, in particular, to assure that principles of personal data protection are fully incorporated in the use and development of information technologies.

The Working Party also has advocated the conception and construction of these systems taking into account and incorporating the technical resources necessary to respect data protection rules.

If we accept that protection will be fully applied, without hesitation, to information technologies, we must determine whether the current community regulations are the appropriate legal instrument.

Directive 95/46/EC Provides the Appropriate System

As I said before, it often is stated that the 1995 Directive does not contain a framework that is appropriate to the new technologies, and that the principles it establishes are irreconcilable with or of difficult application to the processing of information using the systems developed by the new technologies. Again I must disagree with this negative position. For that purpose I would like to address the following aspects.

In the first place Directive 95/46/EC, like many legislative instruments of the Union, is based on the principle of *legislative neutrality*. That is, the system that is established governs all kinds of situations, regardless of the instrument or resource used to process personal data. Because all technical resources that may be used under the directive have the same legitimacy, it does not promote the use of one specific resource over another.

The Court of Justice in its judgment of 6 November 2003 (the Lindqvist matter) confirmed the application of the system under Directive 95/46 to the Internet, specifically to processing of personal data consisting of referring, on a webpage, to various persons and identifying them by name or by a series of criteria making them identifiable.

In the second place, *Directive 2002/58/EC regarding processing of personal data and protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. This document complements the 1995 Directive and establishes a series of specific provisions to assure protection of personal data in the electronic communications sector, as well as free traffic in such data and electronic communications equipment and services in the Community. It specifically refers to the Internet revolution and the need to assure user confidence regarding respect for their privacy as a fundamental aspect of assuring the success of cross-border development of these services. Article 5 of this directive requires the Member States to assure confidentiality of communications and of the message data associated therewith, sent over public communications networks and electronic communications services available to the public. It prohibits listening to, recording, storing and other means of intervention in or surveillance of the communications and the message data associated therewith, without the consent of the users in question, absent an enabling legal provision based on specific reasons of general interest.

This directive is being evaluated by Commission personnel as a part of overall evaluation of the provisions comprising the regulatory framework for electronic communications services. The purpose of this evaluation is to determine whether the system under this directive provides an appropriate framework for protection of the security and privacy of citizens, and promotes consumer confidence in the information society and contributes to the development of the internal market. On the basis of this evaluation the Commission will present the necessary proposals during the course of this year.

In my judgment the current framework continues to be valid. The principles it establishes are well-founded legal principles that may be applied to all kinds of situations, whatever the resource or technique used to process personal data. Perhaps it is necessary to ask how their application can be integrated into the new information technologies. I insist, it is a matter of defining the manner of application of the current regulations to assure protection of the personal data that is processed. It is not a matter of determining repeals of or bases for not applying these principles to the systems or mechanisms developed by the new information technologies.

The Article 29 Working Party, one of the main purposes of which is exactly to contribute to interpretation and homogeneous application of the directive, on several occasions already has opined to this effect. Now I would like to address two recent examples that confirm application of the scheme of the directive to very advanced systems and services of the new information technologies: the e-mail screening system used by providers of e-mail services and the so-called "geolocalization" services.

E-Mail Screening Services

As regards *e-mail screening services, the 21 February report regarding privacy matters within the scope of e-mail screening services* is an excellent example. E-mail screening services (antivirus, antispam, firewall, etc.) are increasingly used by communications services providers. In most cases they respond to the growing concern among providers and users regarding the vulnerability and reliability of the services and systems. Together with these mechanisms seeking to assure appropriate functioning of the communications networks, another kind of screening system is being developed. We might call it "value added" screening. The purpose is essentially commercial: to learn of the kinds of messages from users, file the messages based on their content or the sender, or monitor the handling of the messages by the addressee. All of these mechanisms constitute a greater or lesser intrusion into the privacy of the communications or messages interchanged. In most cases they are undertaken without consent of the user with respect to whom these services are applied.

The Working Party report notes the full applicability of the current directives regarding data protection, in particular Directive 2002/58/EC (e-privacy), to these systems, and examines the various types in light of the principles established by the directives in order to assess their compatibility. I will not now delve into the excellent analysis made of each of the cases. I will limit my self to stating that, on a general basis, when the purpose of the mechanisms is to assure security of the networks and their proper functioning, as well as their reliability and speed, and to assure the provision of the services contracted for by users, the Working Party believes that the use of these mechanisms for screening and monitoring messages will be compatible with the principles of the directive. But in any event it will be necessary to respect the essential principles of disclosure to the user, for example the principle of proportionality, which implies that the examination or screening of the messages must be undertaken in the manner least damaging to the confidentiality of the communications and privacy of the users.

But the Working Party considers screening services the purpose of which is purely commercial (for example monitoring what the recipient did with the message: read it, how many times, forwarded it, to whom) to be incompatible with the directives on data protection. Such services are not justified on any of the grounds contemplated in the directives. They imply abusive and unlawful intrusion into and access to the content of the correspondence behind the user's back. The user is not aware of it and cannot give or withhold consent in this regard. Said services must be applied by making the necessary adaptations therein to incorporate the data protection rules.

"Geolocalization"

Another phenomenon showing the need to reconcile new technologies and data protection is the one known as "geolocalization." There are undeniable advantages of data localization services allowing tracking people or objects and determining their physical location. It must be admitted that in certain cases the use of these systems may involve intrusion into the privacy of persons without their being aware of it. Again, from the point of view of respecting the privacy of persons and their personal data, it is not a matter of preventing use of such technologies. Rather it is a matter of developing them in such manner that they respect the fundamental right to privacy and protection of personal data, and are developed in compliance with the applicable personal data protection principles. This focus is reflected in the Working Party Report of November 2005 on "geolocalization." It sets forth the position of the Working Party regarding application of these systems to tracking and surveillance of minors, and of employees by employers.

Work in Progress

Radio Frequency Identification Systems (RFID)

In the opinion of Commission personnel, this recently developed approach should be applied in analysis of other questions of growing interest presented by new technologies, such as those related to radio frequency identification systems (RFID). These radio frequency identification systems increasingly are being developed and used for all kinds of activities and purposes (public, private, commercial and otherwise). There probably is no recent technological development that poses as many privacy questions as RFID technologies. The constantly decreasing manufacturing cost opens broad possibilities of use and application of

these systems (transportation, hospitals, security and access control, supermarkets) with different purposes. Some of these uses raise no question whatever from the point of view of respect for fundamental rights and privacy of persons. But in other cases the systems do imply a significant intrusion into the private sphere, because they are used to obtain and allow the processing of personal data or items that allow identification of a given person. In addition, in many cases this intrusion is undertaken on a surreptitious and subtle basis, without the person in question being aware of it. For example, the credit cards of certain businesses trace the consumption patterns of their customers, which are then used for various purposes. Or "chips" are implanted in the body of a person to facilitate access to discotheques or control access of personnel to certain departments or areas within an organization. In all of these cases a problem arises regarding use of the RFID technology for surreptitious collection of a significant amount of data regarding that person.

Our first task is to separate the RFID instruments or systems that imply collection and processing of personal data, in the sense of the directives, from those that do not so process data. The RFID instruments that do not so collect personal data are outside the scope of the data protection rules. By contrast when these systems collect personal information of the persons involved they *are* subject to the provisions of the community regulations. This requires determination of what "personal data" is under the definitions in the directives.

The Working Party is actively engaged in this work. Following a first working document of January 2005, submitted to public comment, the Working Party has undertaken detailed examination of the various questions raised by use of RFID technology from the point of view of protection of privacy and data protection. One of the matters arising from public comment has been updating the current legislative framework. The Working Party should publish its opinion during this fiscal year. Thus we expect to have the necessary guidance and recommendations regarding application of the directive to RFID technologies.

Privacy Enhancing Technologies (PETs)

To this point I have emphasized those information technologies that by virtue of their design and purpose represent a risk of invasion of protection of the private sphere of the person. Now I would also like to address those technologies that in fact attempt to strengthen and guarantee protection of the private sphere of persons and their personal data. I am speaking of the so-called "Privacy

Enhancing Technologies" (PET). This kind of technology is designed and conceived to minimize the risks of collection and processing of data regarding persons in their relationships with third parties, in particular when the relationships are undertaken using information technologies.

In general, PET refers to systems that not only assure protection of the private sphere and personal data of users, but also seek to strengthen and increase that protection. From the point of view of community regulation, PETs are technologies that allow assurance that the processing of personal data will be undertaken in accordance with the principles of the Data Protection Directive, without on the other hand decreasing the effectiveness and functionality of the instruments used. The PET concept includes various kinds of products, which makes it difficult to define this category precisely. Some of the products reduce the collection and use of personal data that are not strictly necessary. Other products strengthen the security, confidentiality and integrity of the data collected and prevent access thereto by unauthorized persons. Thus, the risk of manipulation and disclosure is reduced. Ultimately, while some products are conceived independently and may be installed by users on their systems to protect them ("defensive" systems) (for example "spyware" products, or products that allow maintaining anonymity when using the Internet), other products are integrated into a computer system or the architecture of a personal data processing system ("integrated" systems including, for example, the encryption of the messages sent). We all are becoming familiar with these products. As the users and consumers we are, we are interested in assurance of our privacy when using the information technologies to avoid, for example, the reading of our e-mail or the monitoring of our surfing of the Internet.

The development of PETs is also essential to facilitate e-government in Europe, because they provide the necessary confidence to assure their development, as has been indicated by the Commission in its work regarding e-government.

The Commission wishes to promote use of PETs, in particular those technologies or systems that are integrated into information system products, by preference over the independent ones that are acquired and installed by the user himself. The former may offer better protection and assurance to users in terms of protection of personal data.

A question that must be addressed here is the determination of to what extent the scheme of the directive appropriately takes PETs into account. It is clear that these technologies, given their nature and purpose, are included within the scope of the directive, because they assure privacy and security and minimize the collection and subsequent processing of personal data. Now there is no reason to exclude reflection on some specific matters.

Our work schedule contemplates the presentation this year of a Commission Notice regarding PETs. Commission personnel are preparing the document, which reflects the work undertaken over the last three years. The Notice will insist on the need to develop communications and information technologies and products that by their design strengthen protection of personal data and privacy of individuals, without diminishing their functionality. It also should underline the need to raise user awareness of these technologies and promote their use by both public authorities and the private sector.

Electronic Databases of Medical Histories

The last example I would like to address is the formation of online medical history databases. The majority of Member States that have not done so are planning to establish national systems for the storage of medical histories of their citizens. Different kinds of systems may be established, from a central archive system to decentralized systems with online access. Different levels of access to these histories may also be established.

The purpose of such systems would be, on the one hand, to improve the effectiveness of medical treatments through better tracking of patients, and on the other to facilitate management of national health systems and contribute to cost reductions. In the majority of cases the establishment of such systems is the result of a legislative decision.

It cannot be denied that implementation of these systems could result in advantages for both citizens, in terms of higher quality of the healthcare they receive, and for the functioning of the national health systems themselves. The creation of these databases raises significant questions from the point of view of personal data protection. In the first place, they are systems used to process data that are considered to be "sensitive," deserving of special protection.

One of the essential questions of these systems is the role given to consent of the citizen. Is the citizen given power to decide whether he will be included in these databases, or what persons may access his personal data? May limits and conditions be established? What guarantees are offered, and what rights is he given in terms of access to his data, consultation, rectification and erasure?

Directive 95/46 contemplated a specific system for processing of this personal data, which affect one of the most private aspects of the person, his state of health, and also involve the doctor-patient privilege. It is absolutely necessary for these systems to be established in accordance with the rules of the directive, as contemplated in its article 8. Perhaps these systems may be based on the need to

protect a significant matter of public interest, contemplated by national law or the decision of the data protection control authority, provided that there are appropriate guarantees for citizens. In any event, it seems essential to me to have consent of the citizen for establishment and operation of these systems. The Working Party is examining these matters, and I am confident that during the course of this year we will have taken a position in this regard.

Conclusions

As I said at the beginning of this presentation, I have attempted to convey to you the reflections of Commission personnel regarding the new information technologies and data protection, in order to show that they are not mutually exclusive matters. We are in the midst of an unfinished work that will occupy all of us during coming years.

Development of and advances in new technologies are essential for progress, and bring undeniable advantages to both society and citizens. Given the growing possibility that such technologies offer for invading the private sphere, it is essential that they incorporate the right to privacy and protection of personal data.

As I said before, the directive is based on the principle of legislative neutrality. It is capable of governing all kinds of situations, regardless of the instrument or resource used to process personal data, without favouring the use of one over the others. The directive establishes a series of well founded legal principles that must be able to govern all kinds of situations. Falling to the Article 29 Working Party is the fundamental task of developing and adopting recommendations and interpretive guidelines contributing to facilitating coordinated and uniform application of these principles by all of the Member States to assure appropriate protection of privacy and protection of the data of all citizens in all situations.

There are no bad or good technologies. It is their utilization and the use given to the principal factors that determine whether they integrate and respect the fundamental rights of privacy and protection of personal data. Therefore it is essential that from the time of their conception and design they include appropriate mechanisms and devices to respect the principles of the directive regarding protection of personal data. Not only because it is a basic requirement for respect of a fundamental right of the person, but also because confidence in and credibility of the information technologies will be enhanced.

24

Data Protection and New Technologies: "Ubiquitous Computing"

Reijo Aarnio
Data Protection Ombudsman, Finland

Introduction

It is a pleasure and honour for me to participate in this congress. I am also very pleased that my presentation allows me to take a look at the future.
The phrase "ubiquitous computing" in the title of my presentation is quite difficult to define as such. It can refer to the everyday information society, the data processing going on all the time, everywhere. But this idea of omnipresence can even lead to an idea of data processing as something divine. That idea can arouse quite conflicting thoughts and feelings.

The first message of my presentation is that we need extensive and democratic public *debate on values*.

It is true that within the sphere of the EU, particularly under Pillar III, there is debate on the data protection *principles* to be applied, but in addition to that, we should quickly begin the debate on values. Simultaneously, the EU has had several ongoing information society programmes. I think that the current programme is known as the i2010 programme. However, at least in Finland, opinions have been voiced to the effect that the information society development is akin to an old athlete. He knows how things should be done, but does not quite have the energy to work towards those goals.

Because of this, the Finnish Ministry of Transport and Communications—Finland will hold the EU Presidency in the latter half of 2006—commissioned a university research institute, the Helsinki Institute of Information Technology, to produce a forecast extending as far as the year 2015. This forecast will possibly be used as one of the grounds for the new Finnish government platform programme after the parliamentary elections next year. It will also be discussed during the Finnish EU Presidency in conferences and meetings. The forecast was drawn up by 15 researchers from the Institute, each representing different fields of academic knowledge. I can say, even now, that the report sees many good opportunities for accelerating the development and supporting national welfare but it also sees plenty of quite challenging threats.

Technological research is very important for Finland. In the next three years or so, 25 per cent of employed people will retire. There is a risk that our national economy will have to spend its money on the welfare of its citizens, instead of investing in research and development. This, in turn, might lead to the weakening of Finland's excellent international competitive ability. The answer to this challenge is to make the production of services to the administration, business and industry more efficient by the increased use of information and communication technology. Finland has relatively good starting points for this for several reasons. Nonetheless, approximately half of the population is concerned about data security and data protection. Therefore, it is in the best interest of all involved to create systems that the citizens and the business and industry can trust and that are user-friendly and economical. Fortunately, this has increasingly been understood in Finnish society. Data protection has become a success factor for society and business and industry. It has made its way from the fringes of legal science to play a central role in society.

The past and the present

A well-known Finnish politician once strikingly put his great wisdom into a few words: "Prediction, particularly the prediction of the future, is always difficult." When we are embarking on that endeavour, it is well advised to be aware of the historical trends and the current situation.

In the following I will list some key trends in the history of information technology:

— Information technology has always infiltrated its environment;

— It has always reached new users, whose needs have begun to dominate the development of technology;
— Information technology has both destroyed and created professions and industries;
— It has changed and moulded organisations and communities, management and obedience, supervision and the freedom of speech;
— Information technology has changed the way we work and spend our free time;
— It has changed the fundamental basics of the economy; and
— Information technology has deepened the gulf between the world's winners and losers.

However, I want to call to your minds Recital 2 of the Data Protection Directive (95/46/EC): "…data-processing systems are designed to serve man; they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy…" However, we must never forget the Resital's latter part: "…and contribute to economic and social progress, trade expansion and the well-being of individuals."

Indeed, it has become increasingly common to see the significance of integrating data protection into the changing service production chains. We are also pleased to note that the public's awareness of data protection has increased, slowly but steadily. Our understanding of data protection has also improved. Data security is beginning to be seen as a range of means for taking care of the judicial quality of services and other processes. Indeed, each data system is technology, but it also has effects on the realisation of the rights of the various parties.

We understand that data protection and security are always linked to a fundamental process. Data protection legislation as such contains an idea of a life cycle of data processing, from beginning to end. These fundamental processes are implemented with the help of data protection and security. Therefore, the realisation of data protection must always be the responsibility of an organisation's most senior management. These issues are too valuable to be left only to IT experts.

Changing forces

What, then, are the factors that prime us to move on to the ubiquitous computing society? First of all, it must be said that there might not be just one killer applica-

tion that alone would direct the development. Instead, there are many factors, whose combined effect will cause the change. These changing forces include:

— Telecommunications trunk networks will be replaced with optical networks, which have a higher data transmission capacity;
— Simultaneously, the basic technology of wireless local and short-range networks has been developed and their adoption has begun, or has already partly happened;
— Various remote-sensing devices and positioning technologies already familiar to us are also part of our world today;
— All data transmission will shift to Internet-based technology. With the adoption of the new IP address system we will no longer talk about "connecting people" but about "connecting all things and people;"
— Open component-based software architecture will increasingly support many important functions, such as identification, identity management, session management, positioning and information management. Perhaps even confidence (PET);
— XML-based languages enable the compatibility of technologies used by various application areas;
— Small terminal devices will become more common and converge;
— Hidden functions related to technology.

An "internet of objects and their owners" will emerge, and with it, a phenomenon that could be called a "sorting door": a minibar will recognise its contents and their consumption, a washing machine will automatically select a suitable programme and a medicinal patch will measure out the medicine it dispenses. A reading device by the door will identify the person passing through it with the help of a unique RFID combination, but also what that person has in his/her wallet, what he consumes and what he/she is like.

From the users' perspective, the Internet is only a "dumb" network. However, end-to-end connectivity makes different innovative applications on the Internet platform possible. From the users' perspective, openness to these innovations often parallels freedom of speech, transparency of the public exercise of power, democratic principles and active citizenship, but also criminal activity and content. It is currently estimated that the number of blogs (webdiaries) will double in five months. There are currently more than 30 million blogs. Formerly diaries were private and they were kept under lock and key, now they are open for anybody to read.

Ubiquitous society

In a ubiquitous world all activity and movement leave traces. Someone always knows where you are and what you are doing. However, it would seem that criminals are also often able to evade this control—why haven't all virus makers been caught?

In a ubiquitous society the users' activity increases, as does the significance of content created by them. The possibilities for business and industry to offer location-dependent content and services increase. The opportunities presented by profiling will also reach unprecedented levels, because it will be technically very easy to connect personal data with data describing places and objects. We need new technical solutions and a reassessment of legislation to avoid this problem.

Our role as users of technology is rapidly changing. Readers become storytellers, viewers active players, passive listeners become active talkers (even we Finns!), users become developers, consumers producers and subjects participants.

We can also identify the different approaches by the different parties to the ubiquitous society. Terminal device manufacturers will gain added value from new features in the devices and, thus, they keep the prices high. The devices are equipped with properties that the consumers "must have."

We consumers gain added value from rapidly developed and accurately targeted innovative services and content, but we may lose our privacy in the process. Once lost, privacy is almost impossible to regain!

Public authorities are between a rock and a hard place. Everyone should be guaranteed a playing field that is open and promotes competition and innovation. Better services and lower prices bring added value to all of society. On the other hand, public authorities can use technology to make their own operations more efficient, to support democracy, equality, transparency, and to increase dialogue with citizens. But how are they able to take care of the promotion of security, data protection and confidence?

Conclusions

So everything leaves an imprint. It makes it possible to identify users, often even when it is not necessary or permitted. People and data systems can draw different

conclusions about us, the users. But is it something new? Technology has always had its pros and cons. Are we able to tell what they are? Most of all, how will we be able to promote good things and prevent bad ones?

Data protection is a value associated with democracy. Its roots lie deep in human rights and the European values based on them. Ubiquitous computing can, at its worst, or almost certainly, threaten these values. Therefore, data protection must not stand alone in defending our humanity. Instead, we need a value debate penetrating through all of society.

25

United Kingdom Freedom of Information Act

Richard Thomas
Information Commissioner for the UK

The transparency of data protection. The Freedom of Information Act, a new law in the United Kingdom and its relationship to data protection and protection of privacy.

As Information Commissioner and Information Protector of the United Kingdom I am responsible for data protection, but also responsible at the United Kingdom level regarding the Freedom of Information Act 2000 and the regulations regarding the environment pursuant to the directive of the European Union to the extent it relates to information regarding the environment. Our approach is to offer public access to official information and at the same time protect the public's personal information, that is, the information of each person. It is a double role we have in our office, since we seek a transparent and open government. The right to know, the right to knowledge, which is legally guaranteed. It is a matter of disclosing all official information, unless there is a good reason to maintain its secrecy. This is the policy. On the other hand there has been a five-year delay in applying the Freedom Information Act 2000.

The focus regarding freedom of the underlying information is truly a challenge as regards the culture and the fact these secrets lead to knowledge of people. This strengthens confidence in the government and regarding operations

and public expenditures leads to the rendering of accounts with respect thereto. It avoids corruption, avoids mismanagement of funds and dishonesty. It improves the quality of decision making at all levels, a true challenge as it relates to the culture of avoiding unnecessary secrets. It is a defining characteristic of a modern democracy.

And it is important to view it as a fundamental democratic value. Politicians and governmental officials are doing or expressing something in our name, and do so with our money. Thus we have to know the details. We have the right to know at least that there is a good reason for not disclosing it. This reminds us, and it is important, that the government serves the people and not vice versa. The government is there to serve the citizens. Application of the Act was delayed for five years. Its enforcement began in January 2005, some 15 months ago.

The Act provides that any person may make a request related to himself. It also may be a company, or an association, an undertaking. It need not be British. It can even be done from another city. Any person may make a request regarding information held by any public authority. We have made a count. There are some 115,000 public entities in the United Kingdom. It applies not only to government at the national level, but also all elements of local government. It applies to each and every school, each and every university in the public sector. It applies to our entire health service, including the practice of medicine and the practice of dentistry. It also applies to the British Broadcasting Corporation, the BBC. It applies to all British services in all areas, throughout the public sector. And when a request is made to any of these 115,000 public entities, it must respond within 20 working days. And of course it is assumed that the request must be respected because, as we say in English, there is a presumption of disclosure. We must disclose the information unless there is an exception. There are 23 exceptions.

Regarding most of these exceptions, if there is a significant public interest, if there is greater weight favouring making the information public, the public interest prevails over what otherwise would be the exception. And as has been indicated, all of this is binding from a legal point of view. Compliance is mandatory.

Functions of the Information Commissioner in the United Kingdom. If someone raises an objection regarding a request for information he has not received, he may apply to the Information Commissioner. The Information Commissioner decides that the information cannot be disclosed or that the public entity will be required to make the information known, or placed in the public domain. If we have the recommendations, we must apply these practical recommendations when compliance with the law is not adequate.

In general, our function is to see to it that good practices are applied by good government. We seek to educate the public, which is also one of our functions. In the first year we received 100,000 requests, 30% addressed to the central government, 40% to local governments and the rest to a broad range of public interest entities. The requests have been made by members of the public that is by users. We are not talking of the mass media or interest groups, or unions. Rather most requests have come from the general public. 60% of these requests were granted. 80% were at least partially granted. In terms of complaints that have been presented, we are very busy. We have had to handle 2385 cases. 1060 of them have been answered. We have issued 135 decision notices. Many have been handled on an unofficial, informal basis. But in some cases official decision notices have yet to be issued. One hundred thirty five cases like these examples.

For example, when environmental inspectors inspect a restaurant, the information now is in the public domain. That is, you can come to London, go to a restaurant and eat or dine with complete assurance. Detailed budgets of schools are made public. If the department of commerce and industry decides to investigate an undertaking because it is asserted that there has been improper conduct of that undertaking, the details of the investigation also are made public. Recently we have ordered an airport in Northern Ireland to publish its contracts with Ryanair. It was asserted that Ryanair paid the airport for landing there, but not at the European level rate based on the number of planes landed. This proved to be true. It was made public, which is of interest to many countries.

We have asked a university for details regarding its standards, because it was suspected that it reduced standards when awarding university degrees. This has been made public. The public has asked us for information regarding the cameras located on roads and highways to monitor speed. Now we have that information both on paper and electronic maps, but we have not stated what camera is active at a given time, because that presumably would hinder law enforcement.

The Information Commissioner acts in all cases in which it is asserted that there has been misuse of public funds. This information now is in the public domain.

Citizens have requested information regarding cardiologists. We now know the success rate of all cardiologists and surgeons. Likewise regarding subsidies or contributions paid in England and Wales. Everything paid by the European Union has been made public. And, for example, how much the Prime Minister's wife's car costs. The value of the car and how much we pay the driver.

Having all of this information is a challenge. We are in an environment that is not always simple.

But the role of Information Commissioner has two aspects: responsibility for data protection, but also responsibility for freedom of information.

Given these two roles, we may ask whether they are competing or there are tensions as between the transparency to be achieved on the one hand and the confidentiality that must be maintained on the other, which is the core of data protection.

Is there a conflict between this openness on the one hand and the need to maintain secrecy on the other? The answer is a categorical no.

There is no contradiction. In fact these values complement each other. It must be remembered that there is a subtle difference between official information that must be transparent and open and, on the other hand, personal information that must be maintained in the private domain.

These systems are founded on a clear base of information rights. They therefore seek proper management of information. Both are focused on a high level of proper management of records with the highest satisfaction of the best standards, assuring access and transparency in well-defined situations. Both strengthen democratic values.

In many countries in the world, not all but many, there are two officials at the highest level, one responsible for data protection and the other for freedom of information. But I believe the tensions are better resolved if a single official is responsible for both. 50 countries have some form of freedom of information law. It always is necessary to have some exception related to personal information. The United Kingdom has resolved this, from an intellectual point of view, in an ingenious manner, but in practice it is not easy.

The focus, as regards the interface, is an exception. In summary, section 40 of our law provides that there are exemptions. That is, in certain cases it is not necessary to enforce the right to know. This is the case when the information requested is information held by a public entity that refers to personal data that is protected under the data protraction law, disclosure of which would violate the law or the principle of data protection. Therefore there is a close relationship between the two laws. On the one hand, the solid basis of this involvement in both functions is clear within my department.

During this first year we have attempted to make this interface a reality. But it is not always easy to do so. And it is not surprising that in countries where there are two high officials, there are conflicts between them. But we have found ways, principles that distinguish between the public life and the private life of an individual. We are rather impatient when a minister tells us that he cannot say with whom he has recently met, or with what companies, because that is contrary to

the minister's right to protection of personal data. And we have to tell the minister that that is the public life of an individual, not the private life of the minister. In addition, when there are public funds, we believe this is an important principle. It has to be tracked, to see where it goes, how these public funds are used. To the extent we implement these ideas we do what the public expects, making what is done by politicians and officials at the highest levels more transparent.

To the extent people join an organization at a younger age with less responsibility, they have a more private way of undertaking their work. I believe they have a greater right to privacy in such cases. And now we have cases, for example, of an audit based on the fact that certain details were disclosed regarding something very unusual. It involved what had been paid to an official in the public domain, someone who had been hired for just 12 months and had received three times the normal salary. We requested that these details of the contract be disclosed, be made public, because they were public funds, paid by the public entity under this temporary 12 month contract offered to this official.

Recently we also addressed expenses of members of Parliament. This is an area that lends itself to controversy. To date we have requested disclosure of information regarding how much is spent per trip, how much per airplane, how much per road trip, how much per train in Scotland, where there is a slightly different system with a Scottish Commissioner. We seek the expense per individual trip. This creates difficulties for a politician who claimed an enormous number of daily miles because he said he travelled to the Scottish Parliament. In reality he lived nearby the parliament and then said he spent a lot on transportation and he lived there. In fact this particular politician simply had to resign.

By way of conclusion, a government that maintains secrecy is not a healthy government, is not a good government. People in a democracy have the right to know what the government is doing at all levels.

Freedom of information transfers official information to the public domain. This is the power given to the public, to the people. But on the other hand too much information about any of us as individuals held by the state, or by private organizations, also is not positive. If the government retains too much information about us it is a government that does not operate properly. The safeguard of protection of data about individuals results in a particular government not retaining too much information about persons. The safeguard of data protection seeks to avoid what we call the surveillance society.

The conclusion is that a healthy democracy must take both data protection and freedom of information very seriously.

26

Transparency of State Activity and Data Protection

Ewa Kulesza
*Inspector General for the Protection of Personal Data of the Republic of Poland**

The philosophy of democratic states guarantees to citizens the right to information on the activities undertaken by the state authorities and its officers.

The freedom to seek, obtain and disseminate information and ideas, as a right of every man as a member of the civil society, was enshrined for the first time in the Universal Declaration of Human Rights of 1948, which is fundamental for human rights. Despite the fact that this act was not legally binding, its universal nature led to the human rights specified in the Universal Declaration being reflected in the legal acts that followed the Declaration such as the Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 and the International Covenant on Civil and Political Rights of 1966.

Following the above, the right to information is treated as a fundamental right of the European Union, and European legislation specifies the standards for access to public information.

It is also relevant that the right to information defined at the beginning in a general way later, in the course of legal interpretation and also by means of recommendations, resolutions, and decisions of the Council of Europe, worked out

* Position held at the time of the event.—Ed.

the details of obligations of public authorities. Essential meaning in this regard has the recommendation of the Committee of Ministers of the Council of Europe of 1981 on the access to information held by public authorities. For example the recommendation indicates that it is inadmissible to demand the reasons of the legal interest of the person applying for the information, the right to information is based on the principle of equality, the refusal of provision of information must be reasoned or the refusal of provision of information is possible only where necessary in the democratic society because of the reasons specified in the law.

Such right to public information defined and protected by international law allowing for the public control of the operation of public institutions has been reflected in the national legislation of the majority of states of Western Europe. Also the "new" democracies attach particular importance to the right to information. The above results from the fact that in the states of the former regime, in so called socialist states, the citizens were deprived of the right to control the activity of state and its officers. Therefore now the transparency of the activity of state is often enshrined by provisions of constitutions.

Poland is a good example of such a state. Polish citizens have the right to public information enshrined in Article 61 of the Constitution. Pursuant to this provision "[every] citizen has the right to obtain information on activity of bodies of public authority and persons holding public functions." More detailed guarantees were introduced by the Act of 2001 on the Access to Public Information. The Polish act has broadly defined the term "public information" as well as the right to obtain information. According to the Act any information on public matters constitutes public information in the meaning of the Act and is subject to be rendered accessible. In particular the following categories of information are public information in the meaning of the Act: all information on internal and external policy, including intended activities of the legislature and the executive, drafting legal acts, programmes concerning the realisation of public tasks, the way they are realised, realisation and effects of realisation, rules governing the operation of public entities, including the way of operation of public authorities and their organisational units, official documents (e.g. on the course and outcome of control and addresses, positions, conclusions and opinions of entities carrying out the control) and public property. Information on persons holding public functions connected with those functions, including the conditions upon which the functions were inducted and are fulfilled, is also the public information.

The right to information guaranteeing the transparency of state activities is in the Western Europe confirmed by a long standing policy and judicial decisions

and does not raise considerable controversies. A slightly different situation can be spotted in some states of our part of Europe. The lack of tradition of democratic state causes that the right to information is in conflict with other citizens' rights such as the right to privacy and personal data protection. It is my intention to present a few reflections on the said collision, real or virtual as resulting from the misunderstanding of the right to privacy.

It needs to be underscored that the socialist state did not guarantee the right to public information or the right to protection of personal data. The Polish legislation admittedly guaranteed the right to protection of personal interest of human being (based on the Civil Code)—which I had occasion to mention several times during international meetings—but the citizen did not have the right to know what data relating to him or her and what documents are collected by the bodies of public authority nor he/she had a right to control the way his/her data were being processed. The right to protection of personal data (the right to information self-determination) as well as the right to public information was enshrined in the Polish Constitution only in 1997. The Polish Constitution in its Article 51 enshrines the right to personal data protection. This right has been developed and detailed in the Act of 1997 on the Protection of Personal Data.

Relatively short period of guaranteeing the citizens the above mentioned rights causes that those rights are treated differently. Perhaps it is a subjective opinion of a persons involved in personal data protection but in my opinion in Poland as well as in some of the so called *new democracies* the right to public information overrides the right to protect personal data or it is assumed in advance that those two rights are in collision. It is especially apparent each time the information on public persons is to be disclosed.

For example, the transparency of state and its officers' activities was a reason for adoption of provisions obliging the politicians, also the local ones, to submit the so called statements of property. Such statements are posted on the Internet which is supposed to allow for public control of the politicians' property. According to the most recent drafts of the provisions this obligation is to be extended on all persons holding public functions and is to be combined with so-called property vetting (inspection) which should be meant as the obligation to give information on all components of the property together with the information on its source.

It raises a question whether the fight against corruption and the right to public information guaranteeing the transparency of state may be a proper premise of such drastic limitation of the right to privacy protection being a fundamental

right for citizens of democratic state? Whether and in what scope such person may invoke his/her privacy or personal data protection?

The Act on the Access to Public Information determines the limits of the public information. Pursuant to Article 6 of this Act the right to public information is subject to limitations because of privacy of an individual or entrepreneur's secrecy. This limitation, however, does not refer to information on persons holding public functions connected with the fulfilment of those functions, including the conditions upon which the functions were inducted and are fulfilled, and the case when an individual or entrepreneur resign from their right.

However, it seems that in Poland a greater importance is attached to transparency and public information. Therefore in the judicial decisions of the Supreme Administrative Court it was confirmed repeatedly that the remuneration of persons holding managerial posts is public even though the general principle states that remuneration is information covered by the sphere of personal interests of an employee. Allowing for primacy of far-reaching openness can be spotted also in the decisions of the Constitutional Tribunal which admits the right to public information at the cost of the right to privacy and the right to personal data protection especially in reference to the persons holding public functions. For example, the Constitutional Tribunal in 2004 examining the compliance of provisions of an act obliging to submit property statements covering also the property of spouses of public persons with the Constitution did not recognise it to breach the right to privacy of such persons. Similarly the Constitutional Tribunal examining the motion for checking the compliance of provisions on disclosing information on persons holding public functions with the Constitution admitted the disclosure of information constituting the sphere of privacy of such persons ordering only to examine each motion for such information on case by case basis (decision of March 2006).

The drafts of provisions constituting the basis for disclosure (posting on the Internet) of documents collected in the past by special services of the communist state also raise reservations from the point of view of possible breach of the right to privacy and personal data protection. The need for openness of information on persons holding public functions is quoted as the condition legalising the publication of such information on all persons listed in the draft provisions (approximately 100 thousand persons). Draft provisions prepared by various political parties provide for publication of information on documents contained in the archives of the Institute of National Remembrance, together with information concerning the sphere of intimacy on the Internet or provide for a public access to such documents. It needs to be noted that such proposals, despite the common

past, are not broadly accepted in all states that are the new members of the European Union. Examples of Hungary or Germany demonstrate that it is possible to clear accounts with the history and simultaneously guarantee the right to information and the right to privacy and personal data protection.

Those two examples demonstrate that implementation and use of the right to public information and the right to privacy and personal data protection in the new democracies, also talking on the example of Poland, requires the understanding of those rights in such a way to allow for their use without the violation of rights of others, as well as the understanding that those rights are not in collision but are mutually complementing. It takes time especially because those states lack legal and political tradition. Above all it requires that the period of transformation should be ended. The sign of this would be the change of awareness and the way the citizens' rights are viewed. This is most difficult, as the adoption of relevant provisions in this regard, even the European ones, is not enough.

27

Transparency in Data Protection

Luís Lingnau da Silveira
President of the Portuguese Data Protection Commission

The argument

The aim of these few words—a humble but sincere homage to the Spanish Data Protection Agency and my good friend Professor Luis Piñar Mañas—is not to present and discuss the possible balance between the principles of transparency and data protection.

It has a more modest purpose.

And it represents something so simple and obvious that perhaps everyone can agree with it.

Nevertheless, it is a remark that is not always made manifest with sufficient and proper strength.

It consists in pointing out that even inside data protection there are certain moments or aspects of transparency—in other words, that data protection is not absolutely synonymous with secrecy and contrary to openness.

This is not said in the line of those who speak of *privacy as participation*[1]—perhaps, I recognise, without accepting all the possible consequences of the *formula*.

[1] Frederic Debussere, "The European Data Protection Directive: An Eye-Patch for Big Brother and Uncle Sam," in "Privacy and Privacy Rights," Chicago, Sept. 2000.

This point of view is not only ambiguous but also dangerous, as it suggests the possibility of integration or even dissolution of the private sphere in the field of public life.

But, on the other hand, between data protection (protection of information concerning persons) and transparency there is no total opposition—rather, a certain dialectic relationship.

It is in this sense, I think, that Professor Stefano Rodotà spoke, almost ten years ago, of one of the paradoxes of privacy:[2]

> These indications oblige us to revise the outlines usually employed in the sphere of privacy and help us face what might be defined as the paradoxes of privacy. The former comes from the fact that the widening of the protection of the private sphere of individuals about whom information is gathered—thanks to the attribution to them of direct powers of control—has led to a greater transparency in the sphere of the information gatherers, be they public bodies or private organisations. The rules on privacy, conceived to ensure opacity and secrecy for the individual sphere, become the go-between for a more accentuated social transparency.

The (disputable) explanation

The public registries

There are, in the first place, some cases of personal data processing that are, by their very nature, public and transparent.

This is the case of the public registries—concerning types of personal data that are accessible to everyone, without proving any special interest or legitimacy.

These public registries are nevertheless a clear example of personal data processing.

Arts 18.3 and 26.1f) of Directive 95/46/EC make clear that only certain aspects of its regime—namely in the fields of notification and transfer—are not applicable to public registries.

The history of the preparation of Directive 95/46/EC shows clearly that this was the aim of its authors.

---

[2] Sefano Rodotà, "Beyond the EU Directive: directions for the future", in Vie Privée: nouveaux risques et enjeux," Namur, 1997.

And I would like to point out that the Portuguese Data Protection Commission has already had the opportunity to defend this position—affirming that the general data protection principles of purpose and proportionality must also be respected concerning data processed in the public civil register.

This is clearly a situation where transparency appears and even characterizes certain types of personal data processing.

Even the personal data processing is subject to a public register system of this nature, according to article 21.1 of Directive 95/46/EC.

This shows how transparency is a desired characteristic of personal data processing.

This observation also supports my opinion that the most transparent of the means considered in art. 18 of the said directive is the notification to a control authority charged with the duty to maintain such a public register.

Right to information

Concerning enforcement of the right to information, there is also a manifestation of transparency, although of a relatively strict scope.

All the information the controller has to provide, following arts. 10 and 11 of Directive 95/46/EC, is only directed to the data subject(s).

Nevertheless, it can be considered as a case of openness about the processing, its purposes and means.

Right of access

The right of access established in art. 12 of Directive 95/46/EC is, clearly, a right directly attributed to the data subjects—and not to third persons or entities.

Nevertheless, there are special circumstances where according to certain laws or general principles of law, or also as a result of decisions of data protection authorities, authorising exceptional derogations to the rule of finality, persons that are neither the data subjects nor the controllers can get access to the former's data.

This happens, naturally, when there are social or other private interests that are considered more relevant that the secrecy defended by the data subjects and the data controllers.

As an example of major public interest we can cite those laws that give the political parties the right of access to citizens' addresses, included in electoral registers, in order to facilitate the political marketing essential to democracy.

Based also on democratic principles, the Portuguese Commission allowed the candidates to a political party internal election to have access to the addresses of all the members of the party, whose data was controlled by the secretary-general (nevertheless a non-unanimous decision).

From another perspective, and considering now the private interests of persons other than the data subjects, our Commission regularly authorizes the access by third persons to health data of deceased people when they intend to use them in a law suit for medical negligence—considering that access to justice is one of the principal rights in a State of Law.

There are therefore cases of transparency in the access to personal data, although of a limited character.

Publicity as the aim of processing

There are, in fact, several examples of personal data processing whose aim is precisely to give publicity to certain information—or, at least, where openness is a natural characteristic of such processing.

We can, in this perspective, think about phone directories (referred to in Directive 2002/58/EC), and the files corresponding to contests of candidates to an official post or the classifications of students after an examination or school year.

Perhaps more subject to discussion—in their admissibility—are certain blacklists, like the one the Portuguese tax office intends to publish with the names of bad taxpayers. However, if they are adopted—sometimes, even by law—they are certainly personal data processing in the form of public lists.

It seems undisputable that all these cases are examples of openness or transparency.

Other general aspects

It is even not impossible to sustain that there are traces of transparency in the principle of free flows of data within the EU or in all the grounds of legitimating data processing, which are not based on the self-determination of the data subject.

Proposed conclusion

Data protection seems, therefore, not to be a one-sided phenomenon, centered on secrecy and "informational self-determination," but a more complex reality, where transparency also plays a certain role.

This comes from the fact that—like everything related to human life—personal data are defined and only understandable in the context of our relationship with others.

Conclusions of the First European Congress on Data Protection

José Luis Piñar
*Director of the Spanish Data Protection Agency**

Data protection, the Directive and Globalization

Directive 95/46/EC on protection of personal data established a point of departure when it stated that there are at least the following premises regarding processing of personal data:

— Recognition of the right of protection of personal data as a fundamental right that has surpassed the more limited protection of personal honour and privacy. And as it is a fundamental right, processing of the data presupposes the existence of a system of guarantees ultimately respecting the dignity of the individual.
— The search for balance of the need for processing personal information and adopting appropriate guarantees must be a constant in the development of the various models of democratic societies.

* Position held at the time of the event.—Ed.

Nevertheless, protection of personal data from an institutional perspective must be checked against its actual effectiveness. Currently there are pressures tending to erode the set of guarantees allowing protection of personal information. These pressures, on an interrelated basis, arise in three areas:

— That deriving from the growing demand for security, basically related to terrorism and other serious forms of delinquency.
— That arising from the increasing requirement of personal information in the marketplace, because production and distribution processes for goods and services are related to the creation of ever more precise profiles of the habits and customs of citizens, directed at discovering information about people such as their physical location and travel habits.
— The opportunities offered by the development of new technologies and the requirements of governmental transparency.

The principal of finality must be absolutely reaffirmed, including in the business area where complete information regarding customers and respect for the principle of finality in the processing of their information are matters that may be incorporated into business strategies as elements of appropriate quality for obtaining economic return.

Based on all of the foregoing:

— It is necessary to achieve a harmonized regulatory development allowing fulfilment of the original objective of Directive 95/46, that is implementation not interfering with economic activity and having uniform guarantees.
— Similarly it is necessary to intensify the work of the Article 29 Group to define common criteria for application of the standards, particularly with respect to new technological developments.
— Cooperation, transparency and accessibility of the control authorities must be assured to companies, in order to hear their concerns and offer them appropriate solutions.

Data protection and economic activity

Experience in third countries such as the United States and Canada reveals the ever more urgent need to make international transactions compatible with the data protection guarantees. The so-called Binding Corporate Rules involve a pro-

cedure in addition to those established in the European Directive regarding the transfer of data, maintaining an appropriate level of protection within a business group, thus facilitating the flow of information. Ultimately it is a way of meeting legal obligations on a coherent basis, with legal certainty, effectiveness and understanding of the law.

Data protection can only be effective if it is accompanied by development and globalization. Companies need to transfer data to develop their businesses. They need new instruments offering the possibility of making international transfers within multinational companies more flexible and reducing their costs and processing. Nevertheless, these new development instruments must be constructed based on the special characteristics and circumstances of the business group to which they are addressed.

The fight against fraud and data protection

The fight against fraud is more important every day because of the proliferation of new phenomena such as phishing, hacking and the increasingly common identity theft. There are new cases of theft through transactions that are undertaken very rapidly and as a result of which a large number of persons may be harmed.

It is necessary to harmonize economic and legal interests of consumers in this area to avoid an increase in the level of fraud interfering with the use of means of payment other than cash and in person payments. Also there must be legal reforms defining specific crimes adapted to the new forms of computer delinquency. Finally, these initiatives must be accompanied by training for judges and prosecutors participating in prosecution of such crimes, and making accurate information available to the police for the conduct of their investigations, so that there will be no *informatics havens* on an international level.

Finally, we should contemplate the possibility that these initiatives may be complemented by other private initiatives providing citizens with self protection tools, or allowing interchanges of information, always respecting the principles of personal data protection and, in particular, unequivocal consent and finality.

Data protection in the fight against terrorism and organized crime

Terrorism today is a global problem to which a legal solution at the international level must be applied. These measures must always take the principle of propor-

tionality into account, so that fundamental rights are limited to the minimum extent possible. Mechanisms such as Europol, Eurojust and Schengen, the recently approved Directive regarding data retention, and the proposals for interchange of information based on the principle of availability are good examples of the advances in building a Space of Freedom, Security and Justice, advances that must not discard respect for protection of citizens.

The increasing demand for security must be made compatible with the fundamental right of data protection and other complementary rights tied to the dignity of the individual. It is for this reason that, when adopting any data protection regulations, it is necessary to observe the objectives of proportionality, effectiveness and technical limitation in national legislation. The construction of a European judicial system must not destroy the primacy of fundamental rights or exclude effectiveness of the principles of data protection within the scope of the Third Pillar. For this reason it is necessary to achieve balance among all the rights and values in play.

New developments in telecommunications and privacy

It is necessary to determine how and in what manner new information technologies must be developed and used in order for the right of privacy and protection of personal rights to be guaranteed. There is no good or bad technology. But the use given to it must be so balanced that, although the manner in which we work and enjoy our free time may have changed, related rights are not affected because they are values essential to democracy.

Also, special attention must be given to the protection of the right of citizens to public information, the ultimate expression of the principle of governmental transparency, which must underlie the actions of the public authorities.

Closing Address

Luis López Guerra
*Secretary of State. Ministry of Justice, Spain**

Thank you and good afternoon. I would first like to thank and congratulate the organizers for their work in organizing this conference, in particular the Spanish Data Protection Agency, which although from an organizational point of view a part of the State Secretariat for Justice, is an entity that acts with total and absolute independence regarding the matters entrusted to it. I would also like to thank the BBVA Foundation and the Superior Council of Chambers [Consejo Superior de Cámaras] for their participation. All of these entities have hereby shown their firm commitment to and cooperation in supporting and spreading the fundamental right recognized in our Constitution for the protection of personal data. I would also like to congratulate the Ministry of Justice for holding this event, for three reasons. First, for the subjects that have been considered; second, for the representatives who have participated in this meeting; and finally, for the work that has been undertaken, of which I have been advised by the Director of the Data Protection Agency.

Regarding subjects, because clearly for all public authorities and entities that in one way or another are responsible for addressing the protection of personal

* Position held at the time of the event.—Ed.

data from the legislative and administrative point of view, the subjects, the challenges, the innovations that are appearing in the legal context require reflection, analysis and cooperation of public and private entities. There are many innovations in the data protection area that accentuate the problems in this regard, based on the evolution of technology itself, and the evolution of everything to do with communications and information media. In our country we are now beginning a phase of implementation of the national electronic document which will ensure greater facility in the knowledge and broadcast of data. This may result in danger or at least difficulty regarding the position of individuals, not only as regards their fundamental rights, privacy, honour, but also regarding their positions in negotiation processes seeking employment, insurance contracts, etc. Ultimately both you and I are aware of multiple examples in which the position of the individual may be affected. So at this time of technical and technological development, and therefore of legal development, this kind of meeting, this kind of gathering of individuals and institutions seasoned and expert in these matters is really something to appreciate. I can assure you that in the Ministry of Justice we will take the conclusions very much into account.

Together with this aspect it is necessary to note a second element: the representatives taking part in this meeting. The problems deriving from technological development regarding disclosure of data are problems that for some time have affected all governments in many ways. They are not restricted exclusively to the national sphere. Ease of communication means all of these problems related to data protection are of an international nature. I believe we are all accustomed to receiving spam or junk mail in our e-mail. That is, all of these thousands of annoying communications that at times threaten to make even the technology itself useless. But not just that. All of us also know that currently there are not only problems of relationships among countries because actions that threaten personal rights may come from various countries. In addition, from an international point of view, national, international or supranational public entities may also take actions threatening the guarantee of privacy of personal data.

Therefore the need to cooperate in this regard extends to all kinds of local, regional, national and supranational governments. In this regard I would also like to note that we are talking not only of the actions of public authorities, but obviously also this entire question very directly affects private entities, those acting in the economic sphere whose businesses may also be harmed by failure to respect personal data. In this regard I believe cooperation among public and private entities is essential if we wish to effectively maintain not only the rights of individu-

als but also the minimum conditions to assure appropriate functioning of the commercial and services sector.

In the light of these challenges I believe it can be said, based on the information that has been provided to me, that the goal set by the organizers when launching this conference has been more than achieved. Highly respected and experienced experts have dealt with fundamental matters regarding the protection of data in the face of these new challenges. The driving force of the European regulation, Directive 95/46, has been considered. It is fully in force and should be taken as an example to be followed. The effect of regulatory provisions regarding protection of personal data on the conduct of private business has also been considered. New challenges have been covered in the area of security and the necessary balance between security and the safeguarding of the fundamental right of data protection. Also, the need to adapt the unstoppable march of technology, the source of new challenges, to these guarantees of protection of personal data.

If we can consider security to be necessary to protect freedom, it is no less clear that it is precisely the existence of a free system that legitimizes and justifies security measures. Freedom and security are related; the loss of either of them results in the diminishment of the other. From this perspective the maintenance of these control systems regarding data protection is what gives security, gives certainty, gives confidence that a constitutional democratic system may implement the security measures to protect precisely those freedoms. The large number attending this meeting shows the sensitivity and importance of the questions related to these matters. During these three days we have been able to learn of the perspective of the private sector, the representatives of businesses, regarding regulations on data protection and their implications for business. The so-called binding corporate rules are shown to be an innovative and legitimate instrument for providing data protection without erecting barriers to business. Regarding the position of the Government, I should also note that we are fully committed to this approach taking into account both security and the needs of the economy. We are fully committed to the need to foster protection of personal data by incorporating advances, identifying such faults or defects as may have appeared and responding to the new challenges. Therefore, as stated by the Minister of Justice when opening this conference, I wish to repeat our commitment to approving the important regulation implementing the organic data protection act, a necessary regulatory implementation that has been and is subject to extensive debate and reflection with the participation of all of the affected sectors. It seeks to achieve the necessary just balance. I can now tell you that it is in the final drafting phase.

In conclusion, I wish to again congratulate the organizers of the conference, encouraging them to continue their efforts to open new avenues of cooperation, dialogue and training, involving all of the social sectors and allowing the formation of what we might call an authentic political civic culture of personal data protection.

Fundación BBVA

Gran Vía, 12
48001 Bilbao
España
Tel.: +34 94 487 52 52
Fax: +34 94 424 46 21

Paseo de Recoletos, 10
28001 Madrid
España
Tel.: +34 91 374 54 00
Fax: +34 91 374 85 22

publicaciones@fbbva.es
www.fbbva.es

ISBN 978-84-96515-41-3