

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



SPANISH DATA PROTECTION AGENCY
ANNUAL REPORT 2005.
SUMMARY

APPEARANCE

Mr Chairman, Honourable Gentlemen, once more I appear before this Commission to inform you of the required Report that the AEPD must prepare, on this occasion for the year 2005.

However, before I start my presentation, I would like to thank the Chairmanship, the Parliamentary Groups and the lawyers who assist it for their effort in making this appearance possible, as I am fully aware of the quantity and importance of the tasks the Commission has assigned at present.

I am thus going to try to be concise, referring to the most outstanding aspects of the Report; mentioning what has been omitted from its actual content and extending this with up-to-date information on the evolution of matters of greater interest.

SECRETARIAT GENERAL

I shall begin my intervention by referring, as briefly as possible to the material and human resources available to the AEPD in 2005 to perform the duties it is assigned.

The General State Budget assigned the agency an expense budget of just over 7 million euros (7,004,180.00 €), a 25.6% increase on the previous year in which, due to modifications that took place during the year, it eventually reached the figure of 7,390,736.37 €.

At the end of the financial year, the level of execution of the budget was more than 95.25%.

The recognised rights, of the financial penalisations, amounted to 21,105,083.99 €, with a total collection of 9,577,590.99 €, in that financial year as well as in previous financial years.

During 2005, the number of public posts the Agency provided evolved from 89 to 98, of which 61% are women and the remaining 39% men. During that financial year, in staff terms, emphasis is placed on active policies for conciliation of working and family life.

A key event in 2005 was the AEPD moving headquarters. It is now located at calle Jorge Juan no. 6 in Madrid.

The change of seat was mainly due to the unavoidable need to extend the space available for the civil servants serving the Institution and, to the same extent, to be able to adequately attend to the citizens and the entities related to the Agency. Thus, on reaching the end of the previous tenancy agreement, it was not renewed.

I take advantage of this occasion to formally invite the Chairman and members of the Commission to visit the new building.

The Agency has always had a special interest in facilitating communication with the citizens through the Citizens' Service Office.

The figures for this activity constitute a first indicator of knowledge of the data protection regulations and of the concern in this field shown by citizens and the subjects bound to comply with the regulations.

One and another have three channels: telephone, personal and written, to obtain information from the Citizens' Service Office. In 2005, the number of queries remained at a stable figure of about 35,500.

Requests for information through this Service mainly refer to exercise of the rights recognised in the Personal Data Protection Act (LOPD) and, especially, those of cancellation (40%) and access (33%).

The specific interest in these two rights the percentages stated reveal is ratified by and matches the data related to protection of these rights that I shall explain to you later.

Nevertheless, these figures cannot be considered an indication of requests for information from the Agency having come to a halt, but rather, one must conclude that, while that interest is maintained and has increased, it has been channelled through other means, that presumably point to a more mature knowledge of the data protection regulations, such as access to the information available on the web page.

Indeed, in 2005 the Agency web page had a considerable increase in number of hits, going from 580,000 to nearly 850.000 (46%). In addition to this, there is the fact that the average duration of web access per user has risen to an average of 8 minutes 16 seconds (VID, Are there figures from 2004?)

This data shows how in a situation in which the Agency lacks regional branches, the new information technologies constitute an adequate channel to allow the citizens to access the relevant information.

This, in turn, requires ongoing effort by the Agency to maintain the information up to date and innovate it.

In this sense, in 2005, one must point out that the Agency web page had a double “a” access level to help the handicapped to obtain information.

The Report refers to a relevant shortcoming of the web page: the absence of a search engine to provide swift, analytical, exhaustive access to the information. That omission was corrected in 2006.

Finally, inclusion of information in English has been intensified, so the key developments, mainly with regard to regulations, are accessible from third countries.

GENERAL DATA PROTECTION REGISTER

As Honourable Gentlemen know, the General Data Protection Register (RGPD) has its legal grounds in the requisite of guaranteeing citizens the right to information to be able to know who might be processing their personal data and for what purpose; as well as to facilitate exercise of the rights of access, alteration, cancellation and opposition.

The Report I am presenting to the Commission includes the novelty of a figure on the number of times citizens have exercised this right to information or consultation, which came to 780,000 (779,925) in 2005, in a proportion of 80% and 20% with regard to privately and publicly owned files, respectively.

The data available in 2006 show a growing trend in exercise of this right, as on 30 September 2006, the number of queries rose to 835,000.

However, to the extent that the LOPD requires all parties responsible, public or private, to notify their files, the Register is, at the same time, an indicator of the level of knowledge and compliance of the data protection regulations.

From this perspective, I have pointed out on other occasions that, in qualitative terms, that is, according to the major corporations that process personal data, and to the possibility of using computer tools that allow increasingly more precise profiles of citizens to be prepared, the Register may be considered complete and up to date. On the contrary, from a quantitative point of view, a major shortcoming is noted in fulfilment of the obligation to notify by professionals, SMEs and small sized Local Corporations.

Now, I may point out with satisfaction that this shortcoming is on the way to being resolved, as 2005 ended with a total of nearly 651,000 (650,773) files registered, a 40% increase on the previous year, in which there has been a notable increase in professionals and SMEs.

The trend to increase in inscriptions is maintained and accentuated, with the forecast of it reaching the figure of 800,000 before the end of 2006.

Regrettably, that greater awareness in the private sector has not been accompanied, to the same extent, in the Local Authorities. This means that the Agency has had to issue a requirement across the board to Local Governments in districts with more than 2,500 inhabitants (176) that have not yet fulfilled the obligation to notify their files.

The formal requirement has had a reasonably positive effect, as nearly 2/3 of the Local Governments notified have complied, or have taken action in that sense, although, with regard to the remaining third, it has been necessary to commence the

relevant proceedings in 2006 due to breach of the LOPD (**61 proceedings, of which 27 ended in a breach thereof being declared**).

At the end of financial year 2005, one may conclude that the greatest percentages of fulfilment were in the provinces of Andalusia – with Huelva at a 100% level of Local Governments with files registered -, Ciudad Real and Barcelona, while the highest levels of failure to comply are in the provinces of the Regional Governments of Castile-Leon and Castile-La Mancha, as well as in La Rioja and Navarre.

As to the Regional Authorities, a 7.5% increase in notifications has been recorded, notably that of the Regional Government of Andalusia, that has reached second position in number of files registered.

On the other hand, the legal requirement to notify – which in our legal system, on the contrary to other European ones, has no exception whatsoever – imposes development of solutions to facilitate compliance on the AEPD.

In that sense, actions by the Agency in 2005 have been aimed at simplifying the notification forms, reducing them from 13 to 3 pages, that include the most relevant information; to preparation of pre-filled-in models for the most usual files (mainly human resources management, customers and accounting management, tax and administrative) and to development of the remote notifications system of the Agency (NOTA), that has been available since 1 September 2006.

The new system constitutes the first electronic administration activity by the AEPD, in the sense of covering the full notification formalities; monitoring processing and resolution of the inscription, which may be performed on-line, if the party responsible has an electronic signature.

Setting up the system has required creation of the Telematic Register at the Agency.

To present, we may feel satisfied with the receptiveness of the new notification system as, from it being set up, the number of notifications received has come to 1,000.

In any case, and notwithstanding of the results arising from the new notification system, I must congratulate the officers at the General Data Protection Register who, in spite of the considerable increase in the number of notifications and daily operations related to these – reaching an average daily figure of 802 – have achieved six day processing of 74% of the notifications (the LOPD foresees a term of up to 1 month for lack of activity by the Registry to be considered as positive administrative silence).

To the same end of facilitating fulfilment of the legal obligations, in April 2005, the Agency web page published a model guide to prepare the security document, mainly aimed at facilitating this legal obligation for those responsible for small sized public and private entity files. This has been most well received, as nearly 58,000 downloads had been counted by the end of the year.

Lastly, within the scope of activity of the Register, I must point out that during 2005, 45 international data transfer authorisation files were processed. Along with the traditional destinations, such as the United States of America and Latin American Countries, in 2005 there was a notable increase in applications to authorise transfers to countries in the Asian Pacific. The most significant ones are those related to outsourcing services such as telephone customer service and hosting and maintenance of data bases.

SUBDIRECTORATE GENERAL OF INSPECTION

I shall now refer to the Subdirector General of Inspection, in which all the indicators of their activity (inspections, procedures to protect rights and procedures for breach of the LOPD for public and private responsible parties) increased by an average 24% in 2004.

The trend is maintained that most of the inspection actions initiated are due to complaints by citizens, although those ordered by the Director of the Agency, normally due to information in the media, come to 7% of the total.

The presence of parties reporting and reported nationwide is also consolidated.

As to their territorial distribution, the first three places are occupied, in prior inspection actions, as well as in procedures to protect rights and penalisation procedures for those responsible for private files, in the Autonomous Regions of Madrid, Catalonia and Andalusia. Only in the case of penalisation procedures, the Region of Valencia is third, after Andalusia.

From the quantitative point of view, the inspection actions initiated consolidate the increase that took place in 2004, with a further 18% growth; the penalisation procedures also consolidate the increase that took place in the previous year and increase by 42% in 2005, and the procedures to protect rights initiated exceed the temporary drop in 2004 and reached a new historic maximum figure of 579 at the AEPD.

So what do these figures show? I consider, as I have pointed out on other occasions, increasingly more widespread knowledge of the “data protection culture”

among citizens and a major increase in the demand for actions aimed at achieving effective enforcement of the guarantees provided in the LOPD.

However, and I must particularly insist on this affirmation, without one having to interpret this in the sense of there being a relevant level of breach of the law and, it thus being obligatory to declare breaches as, just as highlighted in the Report, there are 34% more file settlements of actions than breaches declared in the penalisation proceedings, following the prior inspection actions. In most cases, this is because sufficient proof is not obtained, that allows the principle of presumption of innocence to be broken.

And what implications does that situation have in the AEPD organisation? It is evident that we are faced with a situation of overwhelming workload of inspectors and recorders that requires an urgent increase in staff levels (*if we do not wish a future lack of effectiveness in enforcing the LOPD cause mistrust among the citizens of the capacity of the Institution to guarantee the principles and rights the Act recognises them*).

Analysis of this data by sectors of activity shows that the greater number of inspections and declarations of breach arises in the telecommunications sector, with 24% inspections and 29% penalisation proceedings.

Within that sector, there continues to be more frequent breach of the principle of data quality, due to the undue inclusion of subscribers as debtors on what are known as common default files, which reach a percentage of nearly 50%.

However, this is followed at an increasingly quite close distance by breaches related to subscription of telecommunications services, either because it is not performed by operators with sufficient guarantees concerning identification and true will of the citizens to subscribe the services, committing the offence of data

processing without their consent; or due to noted fraudulent subscription practices involving deceitful gathering of data, giving rise to severe offences that may be penalised with fines from 300,000€ to 600,000€.

This behaviour mainly affects subscription of telephony and Internet access services.

I wish to draw your attention to this so that telecommunications operators, within the legitimate, necessary competition their activity involves, may maximize their diligence when encouraging new subscriptions.

In that sense, I must emphasise that I have noticed greater awareness of the issue among those operators, and the need to establish additional guarantees in the subscription processes, through meetings held, at their request, with the Agency, to evaluate measures to resolve it.

The telecommunications sector is followed by the financial one (with 19% of the actions), mainly due to undue inclusion of debtors on default files, and advertising through channels other than electronic notification of commercial promotions.

These sectors have traditionally been those that have given rise to the greatest number of claims.

However, along with these, a phenomenon of particular concern to me has appeared, which is the increased number of inspections and commencement of proceedings over offences arising from complaints of data processing by the Public Authorities.

In 2005, investigation activities concerning the Public Authorities amounted to 9% of the total (11%, if one adds those related to the activity of the State Security Forces and Corps) and proceedings for breach of the LOPD have increased 86%.

Within this setting, a positive balance is maintained between the Administrations accused, with 37% of resolutions to commence proceedings, with regard to the General State Administration, as well as the Regional Administrations, and 26% with regard to Local Corporations.

And, even more worrying is the major percentage of offences claimed against the Public Authorities for breach of the duty of secrecy, followed by security related offences, as it shows the lack of diligence in custody and confidentiality of the citizens' data, which it is mandatory for them to provide to those Authorities in most cases.

As to the procedures aimed at protection of the rights of access, alteration, cancellation and opposition that the Act recognises citizens are entitled to (592 completed), the data from 2005 shows that the greater number of claims refers, in this order, to the rights of cancellation (348) and access (276) so, for illustration, it shows that citizens are especially concerned to know what information on them is recorded and to have it disappear.

The Report Chapter on the Legal Office includes the heading of “case law analysis”, that shows the criteria of the *Audiencia Nacional* (a division of the High Court) as the body that reviews the resolutions by the Director of the Agency, concerning the set of procedures to which I have just referred (archive/PS/AAPP and TD)´

That heading emphasises the increase in sentences rejecting appeals filed against resolutions by the Agency.

Thus, of the 86 Sentences by the Contentious-Administrative Court of the Audiencia Nacional, only 12 had the appeals filed fully allowed, a reduction of 9% on 2004, and 5 partially allowed, as in the previous year. On the other hand, 12 Decisions or Sentences handed down by the Supreme Court have either not been allowed, or appeals have been rejected.

The notable increase in the inspection activities I have just mentioned has not prevented continuing development, although with a more limited scope, of prevention policies through the trade related sectorial plans.

As Honourable Gentlemen know, the sectorial inspection plans are an auditing mode for fulfilment of all the principles and rights of the LOPD in a sector of activity previously selected. They are not aimed at declaring breaches, but rather at establishing a diagnosis of the situation of fulfilment, to detect deficiencies and provide recommendations that must be fulfilled to resolve them.

The Sectorial Plan Report on what are known as “employment portals” was concluded in 2005. This includes all the companies (organisations with ends of general interest, employment portals, Temporary Employment Companies, personnel recruitment companies, and human resources and major companies consultancy firms) that use the Internet to gather personal data of job seekers who, due to their variety (identifying particulars, personal characteristics, social, academic and professional particulars, details of employment, hobbies, preferences, etc....), allow fairly precise profiles of the parties concerned to be prepared and, on occasions, evaluations of their personality.

The conclusions and recommendations by the Inspectorate are available on the Agency web page.

Likewise, work has been completed on the complex sectorial inspection of regulated non-University Education, the result of which will be presented before the end of the year, with the following structure:

- 14 reports by the Autonomous Regions (excluding Madrid, Catalonia and Basque Country, as these have specific Regional Agencies) on schools fully or partially maintained / financed by public funds.
- 1 nationwide report (except the Autonomous Regions stated), concerning state schools.
- 1 nationwide report on subsidised and private schools.

LEGAL OFFICE

The specialised advisory activity by the AEPD, that is part of what may be classified as the “prevention policy” of the Institution, has remained stable compared with 2004, consolidating the 41% increase there has been in issue of legal reports since 2002.

In qualitative terms, the matters in which there has been a major increase in the queries raised are related to gathering and processing data from electronic communications and processing of health data which, as Honourable Gentlemen know, have a reinforced protection regime.

The notable increase in queries by electronic communications services operators, which have taken first place among those made, is explained by approval of Royal Decree 424/2005, of 15 April, that develops the General

Telecommunications Act, among other aspects, in the detailed regulation of the required guarantees for processing of personal data and, thus, this affects the scope of competencies of the Agency.

On the other hand, the required reports on provisions of a general nature have increased 25%, compared with 2004. This indicates a continued growth in the sensitivity of the Government to the implications of the data protection regulations on exercise of the legislative and statutory initiative.

Briefly, one may emphasise that the main reports issued affect such matters as prosecution of terrorism and other severe forms of organised crime (Prüm Convention and development rules of the legislation on the financing of terrorism and money laundering), processing health data (Draft Bill of the Organic Act on Health Protection and combating doping in sport – that gave rise to an informative appearance before the Education and Science Commission of the Parliament; Draft Bill of the Act on Guarantees and Rational Use of Medicines and Health Products, Regulations on Blood Donation and Transfusion Centres and Services) and the electronic national identity card (DNI-e).

BALANCE

On the different occasions I have appeared before this Commission, I have emphasised the priority of the Agency to extend and consolidate a true standardisation of the data protection culture.

As stated in the Report “a priority of these characteristics is, due to its very nature, an aim in the medium or long term, especially in such a matter as this in which, in spite of the time that has elapsed since enactment of a first Act that

regulates this fundamental right, ignorance of it was fairly widespread until scarcely three years ago”.

The information I have provided the Commission up to present shows the state of the matter in 2005.

However, in order to appreciate the true dimension of progress in achievement of this objective, it is necessary to view it within a wider time scale.

Standardisation of a data protection culture requires to provide citizens knowledge of the guarantees and rights the Law recognises them so exercising these becomes part of their daily life.

It is also necessary to disclose the data protection regulations among those who must fulfil it, clarifying their doubts, simplifying their obligations, performing preventive actions and providing them greater levels of legal security.

With regard to the Public Powers, that priority must also lead to ensuring that all the regulations that may affect processing of personal data are prepared and improved bearing in mind the implications and effects with regard to that fundamental right.

And in the event of breach of the Act, their effective application must be guaranteed. In the case of breach of the Act, performance of these activities makes it necessary to have the necessary material resources and, above all, staff.

The aspects I have stated are clearly recorded in the First Report by the European Commission on the implementation of the Data Protection Directive of 15 February 2003.

In that document, under the heading of “enforcement, compliance and awareness”, the report suggests, with regard to effective enforcement with the Directive, “the presence of three inter-related phenomena:

- An under-resourced enforcement effort and supervisory authorities with a wide range of tasks, among which enforcement actions have a rather low priority;
- Very patchy compliance by data controllers, no doubt reluctant to undertake changes in their existing practices to comply with what may seem complex and burdensome rules, when the risks of getting caught seem low;
- An apparently low level of knowledge of their rights among data subjects, which may be at the root of the previous phenomenon.”

And it adds that “the supervisory authorities themselves in many Member States are also concerned about this, in particular their lack of resources” and “resource difficulties may affect independence. Independence in the taking of decisions is a sine qua non for the correct functioning of the system”.

Now I would briefly like to explain some significant factors, from the perspective of more than three years as the Director of the Agency:

- The figures of files registered at the RGPD shows the major growth in the last four years, as if one considers that at the end of 1995 there were 224,856 files registered, due to the massive inscription process that took place in its first two years of existence, that the figure had reached 328,649 at the end of 2002, and that it is foreseen to exceed the figure of 800,000 files registered by the end of 2006, we may see that in the period 1996-2002, the net growth is 103,793 files, which amounts to an approximate annual growth of 6.57% for these 7 years, compared with the net growth of 471,351 files and the annual growth rate of 35.75% in the last four years. Comparing these figures, we may confirm that the workload of the RGPD has been sixfold.

Considering that, during 2006, the average daily number of inscription operations was **900**, one must point out that since 2002, this activity indicator has threefold.

- With regard to the information provided through the Citizens' Service Office, 19,940 queries were attended in 2002, while in December 2005, that figure increased to a total 35,512 queries, a 56% increase.
- In relation to the queries to the Legal Office, one must emphasise the major increase during 2003 and 2004, confirmed in the following two financial years. Likewise, the number of queries has evolved from 415 in 2002 to 588 foreseen in financial year 2006 (a 42% increase in this period).
- A major advance in diffusion of the fundamental right has been provided by the web page set up in 2003; a complete renewal of its design and operation to guarantee access to it for the handicapped. This institutional page has had a total 7,585,897 visits during the period 2002-2005.
- As to participation by the Agency in preparing general provisions, the increase has been much more significant, having evolved from the 33 provisions studied during 2002 to the 76 reported during 2005, the forecast for 2006 being 83 provisions, which would be a 152% increase during the period.

In that sense, the provisions analysed refer to a large number of sectors, having become aware of the need to submit not only regulations related to creation of the files for approval by the Agency, but also those which, even though they do not directly develop the LOPD, have an essential influence on it, regulating the processing performed by the public and private sectors.

This has meant that, in many cases, Projects that lacked provisions related to the fundamental right to data protection have come to include specific rules on the matter, or have established referral to the provisions of the LOPD.

- The data related to the activity by the Subdirectorate of Inspection is also significant. It is sufficient to note the following percentage increases:
 - Penalisation Proceedings commenced: 161% (148 in 2002, 387 in 2005).
 - Preliminary investigation actions commenced: 60% (723 in 2002, 1158 in 2005).
 - Proceedings to declare breach by the Public Authorities: 300% (13 in 2002, 52 in 2005).
 - Procedures to protect rights: From the quantitative point of view, except in 2004, when the general volume decreased 17%, the overall calculation increased by 30%.
 - Preventive action in relation to certain sectors (Trade Plans).

During this period, 10 Trade Plans were developed, with the following details:

- a. Common file on asset solvency (2002).
- b. Remote Banking (2002).

- c. Television competitions, games and raffles (2002).
 - d. Population and housing censuses 2001. Companies participating (2003).
 - e. Population and housing censuses 2001. Statistics Institute (2003).
 - f. Hotel Chains (2004).
 - g. National Public Administration Institute (2004)
 - h. Hospital Laboratories and entities that provide them services (2004).
 - i. Personnel Recruitment by Internet (2005).
 - j. Regulated non-University education (in progress).
- During the period 2002 to 2006, the AEPD budget increased by 4,881,123 euros, from 4,571,867 in 2002 to 9,452,990 euros in 2006, which is a percentage increase of more than 100%. That budget increase has allowed the Agency staff to grow more than 60% (60.17%), from 68 posts in 2002 to a total of 113 in 2006.

Special mention must be given to the increase in chapter VI, intended for investment, mainly related to the scope of new technologies, which went from 127,992.99 euros in 2002 to a total 1,124,600 euros in financial year 2006, an increase of 1.138%.

- Another important aspect of the objective of diffusion of the Fundamental Right was to provide the Agency specific distinguishing marks in 2004, by renewal of its logotype and implementation of its own institutional image, which has facilitated identification of the Institution by citizens over its two years of activity.

In addition to this, there is the boost to the publications plan, with a total 16 publications issued in the period, with a global print run of more than 100,000 copies, with especial emphasis on the Basic Data Protection Guide and the two page information brochures that have actively contributed to diffusion of the Fundamental Right.

- Since the end of 2002, 20 Conventions and Protocols have been signed in collaboration with Authorities, Universities and representative entities in diverse sectors of society (the detail is provided in the attached documentation).
- Finally, I must not forget to refer in this balance to a factor that has been a priority for me since my first appearance before this Commission, which is the need to prepare Regulations for development of the LOPD.

Last year, I already reported in detailed to this Commission on the reasons that justify the need to approve this Provision with the fundamental purpose of increasing legal security; as well as concerning the detail of work in progress.

At present, I shall just inform you that, after wide ranging debate with the sectors affected in the most diverse forums, the AEPD concluded a draft Regulation that has been made available to the Ministry of Justice, responsible for the initiative in this matter.

According to the information I have available, the Ministry is at a very advanced stage in the work to prepare a draft to be put before the Council of Ministers.

- The objective of standardising the data protection culture has also been embodied in the institutional relations maintained by the Director of the Agency.

Along with the usual relations with the Ministry of Justice and the State Ombudsman, I wish to emphasise the institutional visits I conducted in 2005 to the Chairmen of the Parliament and Senate, in which I informed them of the activities of the Agency and we exchanged opinions concerning the status of the Fundamental Right to protection of personal data and relations by the Institution with each one of the Chambers.

In this section I shall specifically mention the co-operation with the Data Protection Authorities of the Autonomous Regions.

CO-OPERATION WITH THE DATA PROTECTION AUTHORITIES OF THE AUTONOMOUS REGIONS

Since creation of each one of the regional data protection authorities, the Data Protection Agency of the Region of Madrid, Catalanian Data Protection Agency and Basque Data Protection Agency, in 1997, 2002 and 2003, respectively, institutional relations and collaboration takes place between the General Data Protection Register and the regional file registers. In 2005, those relations were continued through meetings of the work group formed in 2004 in order to establish a homogeneous communication protocol between the RGPD and each one of the regional registers, by defining a system to report information on the register inscriptions, regardless of the technology and based on data exchange and security standards.

During this year, diverse meetings were held at the Data Protection Agency of Madrid in March 2005, and at the Basque Data Protection Agency in December.

Both the conclusions of the meetings, as well as their technical documents have taken into account the project of simplification and modernisation of the Telematic Notification to the General Data Protection Register, which will allow exchange of information on registration of files within the scope of competence of each one of the regional agencies and the RGD to be fluent and for the information to be synchronised so register searches will be reliable.

On the other hand, we have continued the bilateral relation with the Agency of Madrid, which has notified inscriptions, alterations and suppressions of files that had previously been registered on its Register, maintaining the same system has been used in recent years.

Likewise, several ongoing tests were conducted with the Catalanian Data Protection Agency to allow harmonisation of the registers during 2006.

Collaboration with the Basque Data Protection Agency has also continued, providing it the necessary support to set up its Register, including dispatch of the public file inscriptions in its scope of competence to synchronise these in the General Data Protection Register.

Moreover, within this setting of institutional co-operation, the RGD proceeded to inform the respective regional registers of the registry movements in 2005, for files within the scope of competence of each Regional Agency.

Co-operation with the Regional Authorities has also involved inspection actions in which, on occasions, it has been necessary to analyse complex situations in which

those responsible for the publicly held files of their competence and, privately held, of AEPD competence are involved. In these cases, we have managed to provide an adequate solution to investigation needs based on autonomy in exercise of the inspection duties, on co-operation in conveying relevant information and respect for the competence of each Authority when handing down resolutions on the facts investigated.

A clear sign of the proper operation of co-operation relations between one Authority and another have been the positive appraisals by their respective Directors at the recent Meeting organised by the Catalanian Data Protection Agency, held on 4 and 5 October, at the seat of the Parliament of Catalonia.

In all cases, we have all been aware of the new situation arising on reform of the Statutes of Autonomy, in which this Commission plays a fundamental role, and for the need to adapt the co-operation framework to the competence regime foreseen in the new Statutes.

INTERNATIONAL AREA AND CONTEMPORARY MATTERS

The Report for 2005 includes a major section on the international activity of the Agency. This provides Honourable Gentlemen detailed information on the intensity, in terms of quantity and quality, of the actions carried out in 2005.

The Spanish Data Protection Agency conducts intense international activity in Europe, Latin America and the USA, concentrating on its participation in very diverse multinational forums of debate and in supervisory activities and international co-operation in data protection matters.

My presentation will be limited to explaining the fundamental benchmarks in this field and informing you of its status to date, as the main challenges we encounter at present are related to problems raised in the international scope and its repercussion in our country.

Within the activities by the **Latin American Data Protection Network** in 2005, the Fourth Latin American Conference was held in Mexico City on 2nd to 4th November.

The Conference provided three notable novelties:

- Its organisation, for the first time, by a body other than the AEPD, which is the Federal Institute of Access to Public Information (IFAI) in Mexico.
- Participation by a large number of people – nearly 400 between Speakers and those attending – who are not integrated in the Latin American network, which shows the interest in personal data protection related matters in that country.
- The approval, along with the Mexico Declaration of 4 specific work documents on the “Network Structure”, “Feasibility of creating data protection authorities in countries in the Latin American catchment area”, “Access to public information and personal data protection”, and Electronic government and telecommunications”.

In particular, first of these documents is a decisive step forward in consolidating the Network, as it deals with matters related to its nature, organisation and operation.

The Conference also consolidated the methodology of creating specific Working Groups, agreeing to set up two permanent Groups on Regulatory Development and on the “on-line” Network; as well as another two temporary Groups on self-regulatory instruments and treatment of health data in medical records, respectively. The documents prepared by those Working Groups have now been prepared and are available.

The Agency participates - as a representative of the Spanish Government – in the **Working Party under Article 29**, the body that gathers the European authorities with competences in matters of personal data protection control, which I have the honour to be the Vice-Chairman of. The Group has worked last year and this year so far on the following matters:

- Electronic medical records
- Processing biometric data (in passports, identity documents, etc...)
- The electronic administration.
- Need to redefine the concept of personal datum arising from the appearance of new technologies that enable new means of identification (RFID devices),
- The necessary information on those who register Internet domain names (the Whois directories).
- Setting up what are known as binding corporate clauses (BCRs), which articulate a system for international data transfers within corporate groups, adapting to their practical operation with full guarantees.
- Reinforcing the competences of “enforcement” by the Data Protection Authorities.

As to the latter, due to its importance and the role played by the AEPD, I would like to emphasise the work carried out by what is called the ***Enforcement Task Force***, a sub-group that analyses that capacity to apply and enforce the data protection regulations by the Controlling Authorities. The AEPD has led the start-up of the first synchronised national action to control application of the European data protection rules, for which it chose the private health insurance sector due to processing sensitive personal data being a key factor in its activities and due to the impact eventual breach would have on a significant number of people in the EU.

Along with our consultation activity in what is called the First Pillar of the EU, our role in the process of creating an Area of Liberty, Security and Justice (the Third Pillar of the EU) has also been intense. We have examined and reported on some of the measures to combat terrorism and organised crime, with many implications on citizens' privacy.

In this regard, I would like to emphasise that the Agency, along with its European colleagues, has reported and made suggestions during the process of preparing the EU directive on the retention of telecommunications traffic data (finally approved in 2006).

Without our questioning the enormous utility such communication data have to police investigation of terrorist attacks, we however wished to emphasise the need to respect the principle of purpose at all times when processing the data, limiting subsequent use thereof. We also recommend that specific security measures should be foreseen at all times (access control, authorised or restricted access, etc).

All these recommendations by the Data Protection Authorities were included in the final text.

Within that same field, the Agency advises and collaborates with the representatives of the Ministry of Justice who participate in the process of preparing the European Regulation Framework applicable to data processing for police and judicial purposes. This important matter of different regulations at national level (e.g.: the Agency in Spain does have competence over police files, but in other countries, the national data authority is not competent: e.g.: Germany, Austria, etc.) is to be discussed throughout the European Union for the first time, although the regime inherent to the information systems of Schengen, Europol and Eurojust is maintained.

The future Framework Decision (an instrument inherent to the Third Pillar) will close a legal shortfall that now exists in the scope of agile, unhindered exchange of information (of personal data) which is absolutely necessary to combat increasingly more internationalised forms of criminal activity.

From our perspective, that legitimate aspiration is also compatible with respect for the essential principles of data protection. Not only that, both are necessary, as veracity, exactness and security of information (known as the quality principle in terms of data protection) is essential for this to be really useful in criminal investigation.

Outside the European scope and in order to develop our new competences in matters of privacy in telecommunications (attributed by the General Telecommunications Act (LGT) in 2003, and more specifically to combat unsolicited electronic communications, trash mail or *Spam*, we set up a collaboration agreement with the competent body in that field in the United States, the Federal Trade Commission. In February 2005, we signed an Administrative Co-operation Agreement with that Federal Authority to combat Spam. This foresees permanent co-operation between both bodies, exchanging information on regulatory and technological development and also promoting training and education in our respective countries in matters of privacy and data protection. Within that agreement, the AEPD organises a post-graduate seminar on data protection, jointly with representatives of the FTC, at the Law School of Georgetown.

CONTEMPORARY MATTERS

The most contemporary matters are due to the new course transatlantic relations between the US and EU are taking, due to the measures to fight terrorism by the US Authorities.

Implementation of measures by the US Authorities to allow immediate access to all information on people (either travelling in their territory, or performing international financial transactions, etc.) is leading to increasing clashes with the European data protection regulations and solutions must be sought to allow anti-terrorist investigation and fundamental rights to be reconciled.

I shall briefly refer to two specific cases that are still on the debating table:

- **The PNR Case:**

Since the end of 2003, after the 11 September 2001 attacks, the Agency has been dealing with what is known as the PNR (Passengers Name Record) Case, or the transferral to the United States of the personal data of airline passengers bound for the United States.

In the early morning of Friday 6 October 2006, the representatives of the Government of the United States and the Council of the European Union reached an agreement on the content of the Convention that will regulate conditions of that transfer. This fact attracted an extraordinary amount of attention in all the media, but it is not a new matter. It fundamentally consisted of providing an adequate legal basis for a Decision passed by the European Commission in May 2004; as the Court of Justice of the European Communities considered this a matter of the Third Pillar, that must be regulated by an adequate rule (International Convention) not based on a Decision by the European Commission.

By virtue of that Agreement, the Customs and Borders Department of the US will have access to certain data (content of the PNR list) of passengers on flights bound for the US, 72 hours in advance. The data may only be used for investigations into terrorism and serious crime; and it may be shared with other Agencies for the same purposes.

A Joint Committee has been formed to supervise fulfilment of this Agreement and the US has also created an Ad-Hoc Supervisory Office assigned to the US Department of Homeland Security.

- **The SWIFT scandal**

Due to information published in the New York Times in June 2006, concerning mass access by the US Government to personal data in the data base of the company SWIFT Belgium (a European multinational company that manages international transactions), at its operating centre in the US, an international campaign was undertaken by the data protection authorities in 33 countries. According to the European data laws, that is an illegal international data transfer which is not authorised or consented by the data subject, who is also completely unaware that his data is being transferred to others.

In the EU, the authorities co-ordinated our investigations through the WP29 and at our last meeting in September, we analysed the first conclusions by the Belgian Authority, which is the competent authority in this case as, once the appropriate investigations were carried out in Spain, we found that the office of Swift Iberia was only a commercial branch of Swift Belgium, that did not perform processing in Spain and had not been involved in the data disclosure requirements by the US authorities.

The Belgian data protection authority has recorded the existence of unauthorised mass access by US authorities to data stored at an operating base located in the USA that was not foreseen for that purpose, but only for greater security of the computer system (a mirror site was created on another continent in case all the

European systems failed). That access was claimed by the American party to be necessary to investigate financial transactions that might be related to terrorist activities. Pursuant to their anti-terrorist laws (Patriotic Act and Anti-Terrorist Act) forced Swift Belgium to allow access.

The case is not yet closed and has led to commencement of trans-Atlantic conversations to ensure transfers are legitimate and secure.