



**London initiative, Follow up
Workshop on enforcement – 24 April 2007**

QUESTIONNAIRE ON ENFORCEMENT PRACTICES

ANSWERS

CANADA	1
FRANCE.....	8
GERMANY- Office of the Federal Commission	15
ITALY.....	20
SPAIN - national.....	28
SPAIN - Catalonia	34
SPAIN - Madrid.....	36
SWEDEN.....	43
SWITZERLAND.....	47
UNITED KINGDOM	50
EDPS.....	54

CANADA

Please note: We have responsibility with respect to two Acts: the Privacy Act, which came into force in 1983, applies to federal government departments and agencies. The Personal Information Protection and Electronic Documents Act (PIPEDA) came into force on January 1, 2001. PIPEDA applies to organizations engaged in commercial activity, i.e., the private sector.

Although our powers are roughly the same under both Acts, there are a few important differences. For example, under the Privacy Act we can conduct audits. (The Privacy Act refers to reviews rather than audits but we have used the term audits in our responses.) Under PIPEDA we require reasonable grounds to believe that there has been non-compliance in order to conduct an audit. In neither case do we require the consent of the organization being audited.

1. Inspections and audits

Organisational aspects

- Is there a specific department in your authority dedicated to inspections or audits?

We have an Audit and Review (A&R) Branch that conducts audits as part of its core mandate/responsibilities.

Complaint investigations are conducted by the Investigations and Inquires (I&I) Branch. Legal Branch typically becomes involved in enforcement actions.

- If possible, provide staff numbers and budget for enforcement (inspections and audits)

A&R had a budget of \$(Cdn.)1.4 million for fiscal year 2006-2007, with a staff complement of nine employees. While most of these resources are dedicated to audits, the A&R Branch is also responsible for reviewing and providing advice with respect to privacy impact assessments (PIAs) conducted by public sector organizations. The Branch also serves as a reference source for both public and private sector organizations, providing assistance and advice regarding initiatives or issues with privacy implications.

- How many of dedicated staff are technical experts? Legal experts?

The A&R Branch does not have experts with an in-depth knowledge of technical issues such as encryption or communication networks. Where required, the Branch relies upon external consultants/contractors and staff members from other parts of OPC to provide such expertise. We have auditing and accounting expertise in the Branch.

The A&R Branch does not have any legal experts, i.e., lawyers, within the Branch. As required, A&R draws on the expertise of our Legal Branch.

- Does the composition of that department influence the objectives and results of the inspections or audits?

Our in-house expertise brings professional auditing standards to our audits and helps to ensure credible results.

- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

Generally yes, the allocated resources satisfy our objectives. These resources will be increasing in the near future. The Branch profile is expected to increase from 5 to 13 auditors. Even with this increase, the resources remain modest relative to the number of entities that are subject to the Privacy Act and PIPEDA. One of our challenges is recruiting individual that possess both a privacy and an auditing background..

Inspection policy

- Does your office have an inspection or audit policy, with annual selection of priorities and targets? If so, on what basis and how are priorities and targets determined? If not, how do you determine objects for inspection or audit?

Yes, we have a detailed audit plan and an audit strategy. We plan on a three-year basis. The plan is reviewed on a quarterly basis with input from senior management.

We attempt to focus our audit efforts on departments and agencies that pose a higher risk (based on the type and amount of personal information collected and shared), on areas/issues where we are likely to have a significant systemic impact and that are likely to be of high interest to Canadians. In the Commissioner's role as an Officer of Parliament, we also factor in Parliament's potential interest in an audit. On the latter point, Parliament just passed amendments to our anti—money laundering legislation. These amendments require

us to regularly review (every two years) Canada's Financial Transaction and Reports Analysis Centre's (FINTRAC) compliance with the Privacy Act. FINTRAC collects, analyzes and discloses financial information and intelligence on suspected money laundering and terrorist financing activities. (See the examples below of recent and current audits.)

Given that we need to establish reasonable grounds to audit private sector organizations, planning such audits in advance is more challenging. Private sector audits are more likely to be affected by specific events or incidents.

- Do you have a publicly available planning of inspections or audits?

Our audit plan is not publicly available. However, planned audits may be reported in the Commissioner's annual report to Parliament.

- Please illustrate choice of priority areas made recently.

In 2005-2006 we completed an audit of the Canada Border Service Agency (CBSA), with specific emphasis on trans-border data exchanges. CBSA is responsible for customs enforcement and border security. Among other things, CBSA is the agency that receives airline passenger information (API/PNR information) from air carriers entering Canada. We chose to audit CBSA for a number of reasons: the increased focus on border security and enforcement post September 11; the amount and sensitivity of the personal information collected; and public concerns about the federal government's information sharing with other governments, particularly the United States.

We are currently conducting an audit of the federal government's exempt data banks. They are called exempt data banks because the normal rights of access do not apply, i.e., individuals cannot obtain access to information contained in an exempt bank. If an individual requests access, the organization will neither confirm nor deny that it holds information about the individual. The four exempt banks contain sensitive information related to national security and criminal investigations. The Privacy Act provides our Office the explicit authority to examine exempt banks. The audit will assess whether these banks have been properly constituted, i.e., the information meets the criteria for inclusion in the exempt bank. The decision to audit exempt banks was based on several considerations: we have not reviewed these banks for 20 years; the increased emphasis on national security and public safety in recent years; the sensitivity of the personal information held in the banks; and the restrictions placed on access to this information.

In terms of the private sector, we are completing a verification review of the measures implemented by a financial institution following the misdirection of facsimile transmissions containing personal information. We have also initiated audits of two private sector organizations. One of the audit entities, Equifax Canada, is a credit reporting agency.

- Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice.

Most of our resources are typically devoted to “full-fledged audits”. For example, the audit of the CBSA required approximately 4,000 person hours and our exempt bank audit is expected to require 1,000-3,000 person hours. We are planning to begin a pilot program of “site visits” to assess the privacy management frameworks that have been implemented by federal departments and agencies. A complaint or a series of complaints may be a factor in a decision to audit an organization, but we do not initiate audits solely in response to a complaint.

- Similarly, do you make a clear distinction between security audits and privacy audits, or between organisational and IT audits? Please explain your practice.

We do not distinguish between a privacy audit and a security audit. An audit would typically address both privacy issues, e.g., the legal authority to collect information, the management of the information throughout its life cycle (issues surrounding use, disclosure, retention, disposal, etc.), and security issues, e.g., the manner in which the information is protected, the security infrastructure surrounding IT systems, etc.

Recent experiences

- How long has there been an inspection or audit activity in your DPA? If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success?

We have had the authority to conduct audits, technically called reviews under the Privacy Act, since the Act was passed in 1983. We conduct private sector audits under the authority of PIPEDA that came into force on January 1, 2001. Our audit capability has increased significantly since PIPEDA was passed. With our increase in resources we have been able to conduct more thorough audits.

Recognizing that the Office had not used its audit powers to their full potential in assessing the quality of privacy management or addressing the risks inherent in public sector organizations, we are rebuilding and re-enforcing the audit and review functions. We intend to make greater use of audits and they will become an important tool in carrying out our mandate pursuant to the Privacy Act and PIPEDA.

In our view, key factors to success include: developing audit tools (criteria, standards operational methodologies) ; creating well-balanced audit teams that collectively bring privacy, auditing and information security expertise; developing through environmental scanning an in-depth knowledge of privacy-related activities of potential audit entities and emerging privacy technologies; and , conducting audits that will have a positive impact on the management of privacy that extends beyond the audited organization.

- Please provide recent figures, if possible distinguishing between the different types of inspections and audits?

Over the past two years, our available resources have been devoted to four public sector audits, all of which are considered “full fledged” audits. We have also completed one inspection regarding a public sector organization’s use of extension notices. As noted above, we are also engaged in conducting two private sector audits.

- Which inspections or audits do you consider as especially noteworthy? Please describe results and lessons learned.

Our major audit of the Canada Border Services Agency (CBSA) yielded a number of noteworthy findings. The report can be found on our web site at www.privcom.gc.ca. Some of our findings were not made public for national security reasons.

This audit and our review of public information about trans-border data flow generally led us to conclude that better control and accountability is required overall. Greater transparency should be given by government in order to allay public concern about trans-border exchanges of personal information.

2. Sanctions and other measures

Organisational aspects

- Is there a specific department in your authority responsible for sanctions and other measures?

Investigations are conducted by the Investigations & Inquiries (I&I) Branch. Following an investigation into a complaint we issue a report. If the complaint is well-founded, our report includes recommendations directed at the organization that was subject of the complaint. We have initiated a policy to ensure compliance with our recommendations. If an organization does not implement the recommendations within 45 days of the report, the matter is referred to our Legal Branch to pursue litigation.

Under both PIPEDA and the Privacy Act, the complainant has the ability to go to court where damages or other remedies can be ordered. (The grounds for going to court are broader under PIPEDA, for example, the complainant can seek damages under PIPEDA.)

In addition, the Commissioner can initiate complaints.

At the conclusion of an audit we provide the organization with a copy of the audit report. The report typically contains recommendations that are non-binding.

We do not have the authority to issue fines but we can seek damages in Federal Court.

- If possible, provide staff numbers, professional experience and workload.

I&I currently has 39 staff members, 34 are devoted to investigations. In 2006, we completed 309 PIPEDA investigations and in 2006-2007 (we use different reporting periods) we completed 939 Privacy Act investigations. We have a backlog of complaints under both Acts.

Our investigators come from a variety of backgrounds including in the field of human rights as well as law enforcement experience.

- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

Generally yes. One of our persistent challenges is finding qualified people to fill available positions due, in large part to demographics. We are understaffed at present.

Recent practice

- Please provide for recent figures for different types of sanctions and other measures available to your authority?

In 2006, we completed 309 PIPEDA investigations and in 2006-2007 (we use different reporting periods) we completed 939 Privacy Act investigations.

We were involved in 17 court cases in 2006—15 involving PIPEDA and 2 involving the Privacy Act. We were the applicant in 4 cases; an intervenor in 3 and a respondent in 10. Note that some of these cases may have commenced before 2006 and some are still ongoing.

- Which sanctions or measures not yet available to you would be useful?

We are satisfied with the tools we have available. We intend to make greater use of our existing enforcement measures, such as private sector audits.

- Are decisions on sanctions or other measures systematically made public, and if so, how? If not systematically, on what grounds does your DPA make the decision to give the cases publicity?

Typically, we do not reveal the name of an organization involved in a complaint investigation. We release anonymized summaries of a large proportion of our PIPEDA complaints.

- Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof.

In general, we receive excellent cooperation and compliance from a majority of respondents. Our recommendations were accepted and implemented in over 90% of cases in 2006. However, we have been primarily dealing with individual cases rather than systemic issues which we hope to focus on in the future.

- Which actions do you consider as especially noteworthy? Please describe results and lessons learned.

Media attention relative to lapses in the protection of personal information is a strong incentive for the private sector's compliance to our privacy legislation.. Though we do not initiate media reports relative to data breaches we will take the opportunity to comment in order to educate and underline the need for better privacy practices.

Under PIPEDA we will not hesitate to undertake court action to ensure compliance and request remedies when recalcitrant organizations refuse to comply with the legislation.

3. International cooperation for enforcement

The OECD report contains very useful information on that subject and concludes with a number of possible topics for further study. We would like you to consider the following questions, inspired to a large extent by the OECD report:

Note: Commissioner Stoddart is the chair of the OECD volunteer group that has been working on the issue of cross-border enforcement co-operation. We see this as an important priority.

- Has your DPA been involved in 2005-2006 in cross-border enforcement activities? If so, what has been accomplished or learned?

We regularly work with our provincial counterparts on cross-border enforcement issues within Canada.

Internationally, we have been involved to the extent that we have sought assistance from the U.S. Federal Trade Commission (FTC). Specifically, we have sought the assistance of the FTC with respect to a complaint we received against Abika.com, a U.S. based organization that offers a number of services, including background checks, psychological profiles, unlisted telephone numbers and licence plate searches. The complaint involved information that Abika sold about an individual resident in Canada. Our investigation efforts were frustrated by the fact that Abika.com would not respond to our request for the names of Canadian-based sources. As such, we had no means of identifying a Canadian presence for this organization.

A recent Federal Court decision ruled that we had jurisdiction to investigate a complaint against an organization that operated entirely outside of Canada. The Federal Court's decision also highlights (to a certain degree) the practical difficulties we face as we try to investigate an organization that operates outside the country.

As a result of the court decision we have now reopened our investigation of Abika. (Normally, we do not disclose the names of organizations we are investigating—in this case the information has been disclosed through the court proceeding.)

Following the passage of the Safe Web Act by the U.S. Congress, the FTC has clearer authority to share information with other enforcement authorities.

To date, we have not been asked for assistance by other enforcement authorities.

- What would be in your view priority areas for cross-border enforcement cooperation?

Establishing priorities may be challenging, given the limited experience to date with cross-border enforcement cooperation, at least outside the Article 29 Working Group. As a first step, perhaps we should focus on creating cooperation mechanisms and gaining more experience with cooperation.

- Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation?

One of our lawyers is specifically tasked with working with other authorities. As noted above, we have not received any requests for assistance. Given our Office's view on the importance of such cooperation we would make resources available to respond to requests, subject to the demands of our workload.

We are devoting time and resources to furthering cross-border cooperation through our involvement in the OECD's work in this area and we are also involved in a similar initiative with the Asia-Pacific Economic Cooperation (APEC).

PIPEDA, our private sector legislation, is currently being reviewed by a Parliamentary Committee. As part of the review we have asked for an amendment to make it clear that we have the authority to share information with other enforcement authorities.

- Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...)?

Yes. As mentioned above, we have been involved with the OECD initiative that has involved some work on practical tools.

FRANCE

1. Inspections and audits

Organisational aspects

- Is there a specific department in your authority dedicated to inspections or audits?
Yes (created in 2001)
- If possible, provide staff numbers and budget for enforcement (inspections and audits)
7 persons
No specific budget allowed. We are currently assessing the price of each type of audit.
- How many of dedicated staff are technical experts? Legal experts?
2 legal experts (including head of department); 5 technical experts (of which one former policeman)
Other legal experts assist the inspection team for specific inspection
- Does the composition of that department influence the objectives and results of the inspections or audits?
In fact it is depending on the expected difficulty and technicity of the inspection that the team is composed. No inspection was dropped because of a possible shortage of competences in the team.
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?
No : there a clear need for more inspections, and the limiting factor is the insufficient staffing of the department. It is currently estimated that the adequate number of persons in the department would be 30 persons.
(note: it was calculated that if every company of more than 10 employees in France (240.000 in 2006) were to be inspected at least once in its lifetime (in the course of an average life cycle of 20 years), in theory 10.000 inspections should be carried out per year (ie 300 persons needed!)).

Inspection policy

- Does your office have an inspection or audit policy, with annual selection of priorities and targets? If so, on what basis and how are priorities and targets determined? If not, how do you determine objects for inspection or audit?

Yes. Please find attached the audit and inspection programme for 2006 in annex

CNIL makes a formal distinction between “inspections” and “information visits”, which are designed to gain a better knowledge on a specific sector, for instance. In the first case sanctions may be issued, not in the second (the formal requirements to decide that an inspection or such a visit will take place are different – more formal in the first case).

Inspections are usually carried out on the basis of the following reasons:

- *follow up of complaints*
- *follow up of a recommendation issued by CNIL in a specific sector*
- *check that the characteristics of a processing are actually in line with the contents of a notification to CNIL*
- *check of security measures put in place to ensure confidentiality of data*
- *check first online, then on actual site the data protection management behind Internet Websites*
- *check compliance in a specific sector in the context of a coordinated action with other DPAs (cf. Art.29 WP enforcement task force)*

Information visits are usually carried out on the basis of the following reasons:

- *address concerns in the public on a given theme*
- *gain a better knowledge of a specific activity, of a category of applications, or of the processing of a specific type of personal data*

- *Do you have a publicly available planning of inspections or audits?
No. This planning remains confidential and this confidentiality is considered very important for the efficiency of the inspections. This does not preclude the inspected controller from sometimes being informed in advance of the inspection to take place (now less than 10%).*
- *Please illustrate choice of priority areas made recently.*
 - i. *DMP (electronic health files): experimentation of a nation-wide project*
 - ii. *Biometrics: generalisation of biometric systems*
 - iii. *Police files: consequences of 11 september, etc.*
 - iv. *National education (biometrics, CCTV, follow up of violent acts in schools): media attention, nation-wide*
- *Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice.
There is no formal classification, but indeed such qualifications are relevant in practice. Fact-finding visits will be made to follow up of themes considered as a priority by the Commission, including when the inspection is not complaint-based.
Full-fledged audits are not possible at this stage : the inspection department is under-resourced for this purpose. Yet in 2004 CNIL carried out a general audit of Internet banking Websites, which proved very useful and informative. It received good coverage in the press.*
- *Similarly, do you make a clear distinction between security audits and privacy audits, or between organisational and IT audits? Please explain your practice.
Not really.
In the 2006 programme there was a specific item on the check of security measures in specific sectors (namely in the management of electronic health records).*

Of course depending on the inspections the technical aspects may be more or less important. For instance an important item on the inspection programme for 2006 concerned Navigo, the e-ticketing system in the Paris metro and bus network. One inspection led to the inspection of another company, and then to another, etc., because of the important amount of outsourcing done in this sector.

Recent experiences

- How long has there been an inspection or audit activity in your DPA? If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success?

CNIL has always carried out inspections, but few of them before 2001: 324 inspections between 1978 and 2001 (ie 15 inspections per year)

Since 2001 the number of audits has increased. This was made possible with the creation of a specific audit and inspection department. The creation of this department in 2001 anticipated the increase in inspections which directly results from the transposition of directive 95/46 into French law (August 2004).

Indeed the philosophy of the new French DPAct consists in limiting the number of ex ante checks (in principle mostly to sensitive processing), and to increase ex post checks by way of compensation.

This evolution was launched, but is not yet completed. A new organisation is pending to complete this change.

The introduction of sanction powers has in fact been the greatest factor for change in mentalities and perception of CNIL in the public (see under).

- Please provide recent figures, if possible distinguishing between the different types of inspections and audits?

2000: 11

2001: 14

2002: 27

2003: 31

2004: 45

2005: 96

2006: 127

- Which inspections or audits do you consider as especially noteworthy? Please describe results and lessons learned.

Four notable cases in 2006 :

1. *« Navigo » (e-ticketing in the Paris network of public transportation): this series of inspection was decided because of the importance of the issues at stake, ie the freedom of movement of all the travellers within the Paris area (since the system centralises all information on movements inside the network by making use of indirectly identifiable information).*

Main results and lessons learnt:

- *the inspection was complex in technical terms : we did not expect to discover so many sub-contractors, and which is more established all over the country: this type of inspections requires anticipation and an important amount of preparatory work.*
- *The case will be dealt with on May 3rd in the restricted committee to assess the possible pronouncement of a sanction (still confidential).*

2. DMP : Inspection programme in the context of the setting up of the DMP (the French electronic health file)

It was decided that this series of inspections would be carried out on the basis of the importance of the issue for the French society, and in particular with the seven technical providers hosting the citizens' "DMPs" on their computer platforms. This series of inspections focused on a number of issues (conditions for opening a file with each provider, patient's information, access modes, possibility to mask information, security requirements, etc.).

This series of inspections proved very time-consuming, as expected. A lesson learnt from that case, therefore, is that thematic inspections are long and complicated.

This series of inspections implied having recourse to a doctor (a legal requirement under French law to have access to medical files). Interventions in this field prove difficult, as this world is a very close one, very conscious of the importance of the duty of confidentiality.

The most important lesson learnt is that such an important case for the French society as a whole justified to dedicate most of the CNIL resources to the implementation of this series of inspections. Other cases could not be dealt with by way of circumstances, but there was a clear need to prioritise.

3. Joint action of CNIL and HALDE to check compliance with both data protection and anti-discrimination laws

CNIL carried out a series of inspections upon request from the HALDE, the French authority for the fight against discrimination, with a view to checking whether recruitment companies had put in place discriminatory measures when hiring individuals for advertised jobs.

Interestingly, the CNIL was solicited by the HALDE to circumvent the inconvenient that the HALDE is held by law to inform inspected parties prior to its inspections. As CNIL is not bound by such a requirement, this was an advantage for the HALDE. A lesson learnt from this case is that prior information of inspected parties, in particular to research indications of discriminatory information in such files (which may be easily erased if necessary), is inappropriate in practice.

Following this, a specific convention of collaboration was even concluded between CNIL and HALDE for the following purposes:

- *facilitate the exchange of information between the 2 authorities,*
- *carrying out joint information campaigns, joint inspections or joint studies,*
- *mutual training of the staff of both authorities,*
- *appointment of a representative within each authority to facilitate the implementation of partnerships between the two organisations;*
- *regular meetings to facilitate collaboration between the two authorities.*

4. Series of inspections in the City of Montpellier

By the end of 2006 the CNIL carried out a series of inspections during a whole week in the City of Montpellier. The reason for starting such an audit was the finding that this City had filed a substantially lower amount of notifications with the CNIL than cities of similar size. This seemed an indication that the substantial rules of French data protection law were probably not satisfactorily implemented in practice. Indeed this series of inspections, which were carried out nearly as a thorough audit of the city's practices, took more than a whole week to complete.

Eventually, the CNIL issued a compliance order to the City, which acknowledged all its shortcomings. The decision was taken not to publicise the issuance of this order, as it is expected that substantial changes will be implemented soon in practice. CNIL will of course closely monitor this follow up.

2. Sanctions and other measures

Organisational aspects

- Is there a specific department in your authority responsible for sanctions and other measures?

Yes: a specific unit was created in 2006 which is wholly dedicated to the management of sanctions. This unit deals with the whole lifecycle of the cases giving rise to a sanction : it contributes to identify the relevant cases with the other CNIL departments (i.e. the legal, inspection or complaint departments); it drafts the report proposing sanctions (or other options) to the restricted committee¹; it contributes to define of procedures and sanction policy to ensure that the decisions taken are coherent with each other.

- If possible, provide staff numbers, professional experience and workload.
*At the moment only 1 person (former lawyer) is on that team.
2 persons are scheduled for 2007 (including one assistant), a litigation lawyer is the target of this recruitment*
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?
Yes in terms of qualification, but no in terms of resources at the moment, but it should be adequate by the end of 2007.

Important to know: a reorganisation is pending which is designed to improve coordination between the complaints, inspections and sanctions departments namely with a view to better feed the agenda of the restricted committee.

Recent practice

- Please provide for recent figures for different types of sanctions and other measures available to your authority?

After 2 years of activity:

148 procedures

126 "compliance orders" (« mises en demeure »)

15 financial sanctions

9 injunctions to put an end to a processing (ex: no more use of non "opt-in" files for commercial and political emailing)

¹ "Formation restreinte": the restricted committee is a sub-group of the CNIL Commissioners (6 out of the 17 in total) which is the only competent organisation to issue sanctions

14 warnings

Financial sanctions: 228.300€ in total

Crédit Lyonnais: 45.000€

Isorama: 60.000€

Tyco Healthcare: 30.000€

Crédit Agricole Centre France: 20.000€

[Please note that the last 3 figures are still confidential as CNIL has not yet decided whether to publicise these decisions].

- Which sanctions or measures not yet available to you would be useful?

- The main sanctions powers of CNIL (ie injunction to put an end to the processing and financial sanctions) are conditioned by the requirement of the pronouncement of a compliance order. This preliminary requirement can sometimes prove problematic. It prevents CNIL, for instance, from issuing an order to put an end to a processing while carrying out an audit on the spot. It also prevents financial sanctions to be issued immediately, even in case of important breach. This is a clear limitation of the power of CNIL which sometimes acts as a hindrance to the effectiveness of the CNIL's powers.

- The maximum amount of financial sanctions which CNIL may impose (300.000€ maximum, and then only in case of recidivism) is not sufficient for big data controllers; it should be increased.

- Financial sanctions can't be imposed against data controllers in the public sector; this limitation now appears to be questionable under circumstances.

- It is in practice difficult to publicise decisions, which limits the educational dimension of sanctions.

- Are decisions on sanctions or other measures systematically made public, and if so, how? If not systematically, on what grounds does your DPA make the decision to give the cases publicity?

Not systematically. The issue must be considered on a case-by-case basis, since the law requires that the controller is of bad faith to publicise the decision of sanction. This is a limitation in the law which could be usefully changed (see above).

- Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof.

Publicity has a very positive effect on the improvement of compliance by a whole sector of activity. The impact of the publication of the sanction issued against Crédit Lyonnais has had an impact in the banking sector as a whole. It has helped data protection enter the field of compliance issues, so that these issues are handled at a more strategic level than before.

- Which actions do you consider as especially noteworthy? Please describe results and lessons learned.

Crédit Lyonnais : In this case CNIL issued its first financial sanction, which was published in the newspaper and on the CNIL website.

Results: Crédit Lyonnais acknowledged that a mistake had been made, and sanctioned the person at the origin of the breach (other results: see above).

Groupe Accor: this hotel chain had let blacklists being developed by employees, within which a lot of sensitive data would be registered to prevent access to their hotels to clients with reprehensible behaviours. Block note zones were used in an grossly abusive manner. CNIL issued a compliance order which was sufficient to lead the whole group to modify the architecture of its information system (access rights, categories of information registered, storage periods, etc.) throughout the country.

Sector of debt recovery (series of inspections in debt recovery offices and private detectives): we could note that as a whole this sector is well below a satisfactory level of compliance

Additional comment

Indeed this power dramatically changes the way CNIL used to work. It has an impact on all the other aspects of CNIL's work (notification, communication, complaints handling, ...). It imposes greater formalism and compliance with strict procedures (hence a change in mentalities and methodologies). It namely implies that staff in all departments obtains the reflex to propose cases to the sanctions unit, which was not the case before.

It has improved the level of responsibility within data controllers' organisations where data protection issues are dealt with (eg ethics and compliance officers, rather than legal departments only, for instance). It is no easy decision to take: it has possibly huge consequences for controllers; it bears risks in terms of image for DPAs too!; it is indispensable that there is consistency between cases, etc.. In other words, it is a power to use with utmost care.

A real sanction power is a very precious tool for CNIL :

- It compensates the lack of enforcement of DP issues in the courts for want of time, resources, and DP awareness (e.g. on spam)*
- Some cases would not be dealt with otherwise (issues of costs, length of judicial procedures, etc)*
- It helps being taken seriously by data controllers*
- It is very good in terms of communication & awareness raising*

3. International cooperation for enforcement

The OECD report contains very useful information on that subject and concludes with a number of possible topics for further study. We would like you to consider the following questions, inspired to a large extent by the OECD report:

- Has your DPA been involved in 2005-2006 in cross-border enforcement activities? If so, what has been accomplished or learned?

Few cases, dealt with by the complaints department. No specific inspection carried out on the basis of a complaint brought by a foreign counterpart, and no specific sanction pronounced in such cases.

- What would be in your view priority areas for cross-border enforcement cooperation?
 - Spam
 - Exchange of information in international cases like SWIFT
- Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation?
Not specifically, but these cases are dealt with as priorities.
- Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...)?

Cf. OECD work on the issue: CNIL contributed and finds these developments helpful.

GERMANY- Office of the Federal Commission

General information: *The answers refer only to the situation at the office of the Federal Commissioner for Data Protection and Freedom of Information monitoring federal agencies and companies providing telecommunication and postal services. We have not included information about the situation in the 16 federal states in Germany. In the latter range 16 Commissioners of the “Laender” monitor the Laender authorities incl. local authorities and Laender supervisory authorities for data protection monitor private sector entities.*

1. Inspections and audits

Organisational aspects

- Is there a specific department in your authority dedicated to inspections or audits?

No, there is not. Every department is responsible for inspections and audits which fall in its field of activity.

- If possible, provide staff numbers and budget for enforcement (inspections and audits)

Not applicable, because an itemisation is not possible (total staff number (BfDI): 67; total budget: 3,807 Million €).

- How many of dedicated staff are technical experts? Legal experts?

Not applicable, because an itemisation is not possible (BfDI total staff numbers: 23 legal professionals, 8 IT professionals, 36 support/other). Most Länder-DPAs also have staff with legal and technological background.

- Does the composition of that department influence the objectives and results of the inspections or audits?

Such department does not exist (see above).

- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

No, they do not. The human and budgetary resources could be improved. However, the DPA's staff is highly qualified and motivated.

Inspection policy

- Does your office have an inspection or audit policy, with annual selection of priorities and targets? If so, on what basis and how are priorities and targets determined? If not, how do you determine objects for inspection or audit?

There is an annual working plan for the whole DPA relating to inspections and audits. In this context the several departments notify their planned inspections and audits to the head of the agency. Selection criteria relating to objects for inspection and audits are mainly:

- 1. Where there are indications for problems relating to data protection.*
- 2. Where there has not been an inspection or audit for a longer time?*
- 3. How far high sensitive data are affected and how many individuals are concerned?*

- Do you have a publicly available planning of inspections or audits?

No, we do not. The annual working plan is only intended for internal use.

- Please illustrate choice of priority areas made recently.

See the above-mentioned criteria.

- Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice.

Inspections and audits can be (optional)

- 1. informatory*
- 2. consulting*
- 3. policing.*

But in most cases a differentiation is not possible (mixed character).

- Similarly, do you make a clear distinction between security audits and privacy audits, or between organisational and IT audits? Please explain your practice.

This depends on the kind of inspection. During regular inspections all aspects are checked (legal, technical, organisational). In other cases we are focusing on specific issues (f.e. use of customers data for scoring purposes)

Recent experiences

- How long has there been an inspection or audit activity in your DPA? If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success?

Since establishment of Federal DPA in the year 1978.

- Please provide recent figures, if possible distinguishing between the different types of inspections and audits?

In the year 2006 85 regular inspections and audits have been carried out by the BfDI.

- Which inspections or audits do you consider as especially noteworthy? Please describe results and lessons learned.

Most of the work were routine inspections or audits. But two special duties have to be mentioned:

Before the World Cup 2006 in Germany last year the Federal Commissioner has coordinated the work of the German DPAs. Subject was the reliability checking of the people attending the World Cup.

A written survey has been started about the procedure of the credit assessment at telecommunication companies. A questionnaire was send to more than 20 companies.

2. Sanctions and other measures

Organisational aspects

- Is there a specific department in your authority responsible for sanctions and other measures?

No, there is not. Because the Federal Commissioner for Data Protection and Freedom of Information can only lodge rebukes (in § 25 German Federal Data Protection Act referred to as “complaints”). However, the German Federal Data Protection Act foresees administrative offences and criminal offences, but the Federal Commissioner for Data Protection and Freedom of Information is not responsible for imposing such sanctions (other authorities, in particular the prosecution, are responsible).

- If possible, provide staff numbers, professional experience and workload.

Not applicable.

- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

Our resources do not.

Recent practice

- Please provide for recent figures for different types of sanctions and other measures available to your authority?

As mentioned above there are only formal rebukes.

- Which sanctions or measures not yet available to you would be useful?

It would be noteworthy to consider the possibilities of imposing sanctions and giving instructions in case of infringement.

- Are decisions on sanctions or other measures systematically made public, and if so, how? If not systematically, on what grounds does your DPA make the decision to give the cases publicity?

Rebukes are made public in the biennial Report of the Federal Commissioner for Data Protection and Freedom of Information (appendix No. 3).

- Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof.

Rebukes are normally effective, despite their missing legal bindingness, because of the moral authority and expertise of the Federal Commissioner for Data Protection and Freedom of Information.

- Which actions do you consider as especially noteworthy? Please describe results and lessons learned.

For the last two years there have been 6 rebukes, which are not especially noteworthy in this context.

3. International cooperation for enforcement

The OECD report contains very useful information on that subject and concludes with a number of possible topics for further study. We would like you to consider the following questions, inspired to a large extent by the OECD report:

- Has your DPA been involved in 2005-2006 in cross-border enforcement activities? If so, what has been accomplished or learned?

Our DPA took part in a co-ordinated EU-wide investigation into the processing of personal data in the private health insurance sector. In addition, our DPA takes part in a Case Handling Workshop.

- What would be in your view priority areas for cross-border enforcement cooperation?

1. *medical sector*
2. *banking sector*

- Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation?

Yes. The Federal Commissioner is member of a special working group for international data traffic of the so called "Düsseldorfer Kreis" (group of the data protection commissioners for the non-public sector).

- Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...)?

No, we do not (depends on individual case). In particular there is no need for a new network of enforcement officers, because the Case Handling Workshop exists already

ITALY

1. Inspections and audits

Organisational aspects

- Is there a specific department in your authority dedicated to inspections or audits?
Yes, there is a department within our DPA in charge of “Inspections and Sanctions”.

- If possible, provide staff numbers and budget for enforcement (inspections and audits)

The staff of the Department currently includes the head plus two officials. They are supported by inspectors from the Financial Police (Guardia di Finanza). It should be pointed out that the Garante avails itself of the co-operation by the Guardia di Finanza; there is a “Special Civil Service and Privacy Squad” operating within the GdF, working as a unit specialising in oversight activities with regard to personal data protection. This Squad is in charge of carrying out on-the-spot inspections upon the Garante’s instructions. To enhance data protection and privacy know-how among GdF staff, a training programme was started with the help of the Garante; about 140 officers and inspectors from the GdF have taken part in this programme so far.

- How many of dedicated staff are technical experts? Legal experts?

Whenever it is necessary to access IT systems, the Department avails itself of the collaboration provided by the IT Department within the Garante (in particular, two staff members with high-level qualifications and skills). It is expected that additional skilled resources will be recruited in future for the IT department. If the inspection to be performed requires specific legal know-how, staff from the competent legal departments is included in the inspection team.

- Does the composition of that department influence the objectives and results of the inspections or audits?

No, because the inspection Dept. avails itself of the skills and contributions coming from all departments and services within the Garante, depending on the nature and scope of the inspection. Additionally, the peculiar configuration of the oversight framework brought about by our co-operation with the GdF allows performing more inspections than would be possible if the human resources employed by the Garante were only available.

- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

Actually, the resources of the inspection department will have to be enhanced in the next future in order to boost inspection activities.

One of the main priorities pursued by the Garante over the past two years was to increase the staff and operational capability of the inspection department. The 2007 Budget Act enabled the Garante to increase its staff by about 25 units, and our apportionment was increased as well. This was meant in the first place to allow the Garante to better discharge its institutional tasks with particular regard to inspection and controls. The Garante has invested considerably into this sector, as also shown by the new Memorandum of Understanding that was undersigned in November 2005 between the Garante and the GdF. Cooperation with the GdF is fundamental because it allows the Garante to avail itself of skilled resources. Additionally, the GdF can report to the Garante on any circumstances and/or situations that have data protection implications as they are detected in the course of standard control and inspection activities.

Inspection policy

- Does your office have an inspection or audit policy, with annual selection of priorities and targets? If so, on what basis and how are priorities and targets determined? If not, how do you determine objects for inspection or audit?

In addition to the enforcement activities related to the Garante's participation in working groups and task forces at European and international level (see point 3 below), a planning policy was recently developed whereby the panel of the Garante sets out the inspection policy on a six-month basis. The policy specifies the individual sectors to be addressed as well as the scope of the inspection activities including the number of inspections to be carried out for the individual sectors.

Priorities and targets are also determined on the basis of the reports and claims lodged by citizens via complaints and other channels, or else with a view to establishing compliance with the measures taken by the Garante in specific areas.

- Do you have a publicly available planning of inspections or audits?

The general outline of the inspection policy is publicly available, however the number and scope of the inspections to be carried out are not disclosed. It should be emphasized that no audits – meaning a type of assessment that is aimed at establishing the overall data protection compliance of a given system/database – are currently carried out by the Garante.

- Please illustrate choice of priority areas made recently.

In-depth inspections were carried out recently with regard to telecom operators following several cases that were covered extensively by the media and appeared to suggest that access to traffic data was not supervised adequately. A broad range of activities were implemented. They were aimed in the first place to check in concrete how and whether those operators had taken suitable measures to protect traffic data and reports. It could be established that the system for logging accesses to the relevant databases was inadequate and there were no suitable tracing and identification devices in respect of the individuals authorised and/or enabled to access such databases. Careful analyses were also carried out in respect of the mechanisms used by telecom operators to comply with the wire-tapping requests coming from law enforcement authorities.

An inspection plan was also developed with regard to telephone marketing activities carried out by call centres. This was considered to be necessary also further to the many complaints and reports lodged by citizens.

Generally speaking, we believe that one of the main tasks to be discharged currently by our DPA consists in focusing on the security of major databases and subjecting such databases to more stringent, in-depth supervision. This applies, in particular, to the databases related to telecom traffic, law enforcement and ordre public, and the processing of biometric and DNA information.

- Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice.

It should be pointed out that most inspections were carried out up to a few years ago on the basis of the complaints, claims and/or reports lodged by citizens. Currently inspections are mostly performed at the department's initiative on the basis of the six-month inspection policy.

As regards categories of inspection, it should be recalled that the Garante is empowered to request not only data controllers, but also data processors, the persons in charge of the processing, and third parties to provide information and produce documents. Rendering untrue statements and/or communications, or providing forged documents and instruments, to the Garante are considered by the Code to be criminal offences.

More specifically, the Garante is empowered to order that access be allowed to databases, archives and/or registers and may also order inspections and controls to be carried out at the premises where the processing is performed or investigations are to be carried out in order to verify compliance with personal data protection legislation. Such controls are performed by staff from the Garante, who may avail themselves, where necessary, of the co-operation provided by other public bodies. If they concern dwelling places, an authorisation by the geographically competent court is required.

A specific procedure is envisaged by the law (section 160 of the DP Code) in respect of inspections and controls concerning intelligence and security services. In particular, the enquiries are performed by a member of the panel of the Garante, entrusted with this specific task; if the processing is found to be in breach of legislative/regulatory provisions, the said member shall draw the data controller's attention to the amendments required in order to bring the processing into line and will subsequently check that the said amendments were implemented. The member in question may inspect the relevant documents and instruments and must report on them orally to the panel of the Garante; if necessary on account of the specific investigations, he may be supported by specialised staff, who are bound by confidentiality obligations.

If the enquiries are carried out at the data subject's request, the latter must be informed in any case as to their outcome – subject to State defence and/or security requirements.

- Similarly, do you make a clear distinction between security audits and privacy audits, or between organisational and IT audits? Please explain your practice.

There is currently no specific distinction between the inspections concerning compliance and security measures and those focusing on organisational and IT issues. The different issues related to the inspection may be dealt with either jointly or separately depending on the specific objective that is pursued.

In particular, there are inspections in which compliance with organisational and technical requirements is assessed jointly with the performance of a technical audit (e.g. in the case of the inspections concerning telecom operators, see above); conversely, there are less complex cases in which the scope of the inspection is focused more closely on compliance with individual requirements (e.g. provision of information and consent, notification to the Garante, security measures, etc.).

As a rule, especially complex controls are carried out directly by the Inspection Department, whilst more standard ones are committed to the Financial Police.

Recent experiences

- How long has there been an inspection or audit activity in your DPA? If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success?

Inspection activities became formally a part of the organisational framework of the Garante as from 2001. The number of Inspections has been increasing over time with the growing awareness shown by citizens of their own rights, which is also confirmed by statistics on the proceedings instituted by our DPA in this area. The increase in both number and pervasiveness of the inspections was especially remarkable starting from 2005.

Year	2002	2003	2004	2005	2006
Inspections	40	69	100	230	350

- Please provide recent figures, if possible distinguishing between the different types of inspections and audits?

The following inspections were carried out in 2006, broken down by sector:

- 49 inspections concerning public and private bodies using video surveillance systems, to assess lawfulness of processing and compliance with the guidelines recently issued by the Garante in this sector;
- 30 inspections concerning financial consultants and securities brokers, to establish how they processed customers' data with particular regard to profiling activities;
- 28 inspections concerning companies issuing loyalty cards, to assess compliance with the provisions made by the Garante in a provision dated 25 February 2005 (doc. No. 1109624 at www.garanteprivacy.it);
- 26 inspections concerning real estate agencies to assess whether customers' data were processed fairly and the requirements applying to information notices and consent were abided by;
- 25 inspections concerning hotels with wellness centres to assess how they processed data – including sensitive data – related to their customers;
- 20 inspections concerning major museums attracting also international visitors and using video surveillance systems, to verify compliance with, in particular, the obligation to provide information notices;
- 20 inspections concerning public and private social security bodies and agencies to verify compliance with minimum data security measures;
- 20 inspections concerning medical centres and laboratories to verify what measures had been taken in respect of the processing of sensitive data and the notification to the Garante;
- 20 inspections concerning funeral houses to assess how personal data were collected and whether data protection requirements were also complied with during online (Internet-based) transactions;
- 18 inspections concerning telecom operators with regard to the processing operations performed upon activation of services/subscriptions by accessing the data held by private credit reference agencies as well as in respect of the processing related to management of telephone and IT traffic data;
- 13 inspections concerning private exam preparation centres to assess how they processed customers' data;
- 11 inspections concerning companies that had notified termination of processing operations to verify compliance with legal requirements applying to termination of processing, with particular regard to the assignment of the respective databases to third parties;
- 8 inspections concerning companies dealing with personnel selection via certified ads to assess how they processed the candidates' CVs and whether other legal requirements were complied with;
- 5 inspections concerning religious associations to verify what data they processed and in what manner.

- Which inspections or audits do you consider as especially noteworthy? Please describe results and lessons learned.

Special importance should be attached to the inspections concerning telecom operators, as explained above.

The Garante also started an inspection exercise with regard to the data processing centre at the Public Safety Department that is attached to the Ministry for Home Affairs. Initially the inspections were aimed at establishing what provisions had been made to protect the information stored in the relevant databases; the Garante issued a decision to set out measures aimed at strengthening the applicable security measures.

As well as the sanctions imposed on the basis of the findings arising out of the inspections, 25 proposals were put forward by the Inspection Dept. to impose bans and/or requirements on data controllers so as to bring processing operations into line with the law; accordingly, the panel of the Authority adopted especially important measures by having regard to the safeguards to be implemented.

Reference can be made in particular to the following::

- *Measures taken against telecom operators with regard to their accessing information on customers' creditworthiness and reliability (dated 4 May 2006, nos. 1302339, 1302373, 1302385, 1302395 at www.garanteprivacy.it)*
- *Measures taken against two companies managing credit information systems (CRAs) following controls carried out to establish compliance with both data protection legislation and the code of conduct applying to private CRAs (dated 4 May 2006, nos. 1302311 and 1302326 at www.garanteprivacy.it);*
- *The ban imposed on a hotel chain against the unlawful profiling of customers' habits (dated 9 March 2006, no. 1252220 at www.garanteprivacy.it);*
- *The ban imposed on a publisher against the collection of personal data for marketing purposes from maternity clinics (dated 7 December 2006, no. 1379101 at www.garanteprivacy.it);*
- *Two decisions setting out the requirements to be met in order to streamline the processing of personal data related to citizens using e-tickets at Rome and Milan (dated 6 September 2006, nos. 1339692 and 1339531 at www.garanteprivacy.it);*
- *The ban against the processing of personal data collected to issue loyalty cards and used unlawfully also for marketing purposes, following the inspection carried out at a major retail company (dated 24 May 2006, no. 1298784 at www.garanteprivacy.it).*

2. Sanctions and other measures

Organisational aspects

- Is there a specific department in your authority responsible for sanctions and other measures?

In organisational terms, experience has pointed to the need for merging inspection and sanctioning activities as also related to the relationship with judicial authorities – in particular with a view to expediting the procedure for the imposition of sanctions, which requires the co-operation of several organisational units.

The Inspection Department was also entrusted with the task of handling the procedure related to the so-called “remedial action” as regards the failure to take minimum security measures – which is punished by a criminal penalty under section 169(2) of the Code. Based on this procedure, once it is established that a data controller has failed to take the security measures considered as a “minimum” by Annex B to the Code, the Garante sets out the requirements to be met by the data controller in question with a view to restoring the minimum security level set out in the law. If it is established that such requirements have been complied with, a proceeding may be instituted whereby the data controller is allowed to pay one-fourth of the maximum fine provided for by the law and the offence is extinguished accordingly.

- If possible, provide staff numbers, professional experience and workload.

The staff in charge of sanctioning are the same as also deal with inspections. Some figures are provided below:

<i>Year</i>	<i>2002</i>	<i>2003</i>	<i>2004</i>	<i>2005</i>	<i>2006</i>
<i>No. of sanctions imposed</i>	<i>46</i>	<i>27</i>	<i>27</i>	<i>94</i>	<i>158</i>

- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

The increase in inspection activities resulted into a corresponding increase in sanctioning, as shown by the above figures. Hence, additional resources (both human and budgetary) are needed in this area as well .

Recent practice

- Please provide for recent figures for different types of sanctions and other measures available to your authority?

The administrative sanctions imposed, amounting to minimum 601,000 Euro and maximum 3,606,000 Euro, were related to the following offences:

- *failure to provide information notices (133);*
- *failure to notify the processing to the Garante (17);*
- *failure to comply with requests made by the Garante (8).*

The sanctioning system under the Code is two-tiered, as it includes both criminal and administrative measures.

Unlawful processing of data; rendering untrue statements and/or submitting untrue notifications to the Garante; failure to take minimum security measures; and the failure to abide by measures issued by the Garante are considered criminal offences. Conviction for any of the criminal offences set out in the Code entails publication of the relevant judgment.

In addition to criminal offences and penalties, there are administrative offences under the Code. In this case the Garante is empowered directly to impose the applicable sanctions.

In particular, administrative sanctions may be imposed if the information notice is not provided or is unsuitable; if no notification is submitted to the Garante as required; and if documents and/or information are not provided or made available to the Garante.

- Which sanctions or measures not yet available to you would be useful?

The Garante called for regulatory amendments with regard to inspection mechanisms and sanctioning powers as also related to the power to issue specific requirements.

In particular, it would be necessary to empower the Garante to impose administrative pecuniary sanctions to a greater extent and in a much larger number of cases compared with the current situation under the Code. Indeed, one of the main limitations affecting the sanctioning system under the DP Code consists in such sanctions being mainly of a criminal nature.

- Are decisions on sanctions or other measures systematically made public, and if so, how? If not systematically, on what grounds does your DPA make the decision to give the cases publicity?

As regards administrative violations, publication of the injunction order in one or more newspapers – in whole or in part – may be provided for as an ancillary sanction.

As regards criminal offences, conviction entails publication of the relevant judgment as an ancillary measure.

- Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof.

- Which actions do you consider as especially noteworthy? Please describe results and lessons learned.

It might be appropriate to enable the Garante to differentiate sanctions depending on the seriousness of the underlying violations, the collaboration afforded by the entities involved, and the level of compliance with the deadlines set for implementing the measures imposed.

It would be appropriate to introduce an administrative, rather than criminal, sanction in case data controllers fail to comply with requirements imposed by the Garante.

3. International cooperation for enforcement

The OECD report contains very useful information on that subject and concludes with a number of possible topics for further study. We would like you to consider the following questions, inspired to a large extent by the OECD report:

Having participated in several co-operation and co-ordination initiatives at European and international level, the Garante could contribute to international co-operation for enforcement purposes. An example is provided in this regard by the Enforcement Task Force set up within the framework of the WP29; here the participating DPAs carried out a synchronised enforcement exercise with regard to private medical health insurance. Additional experience could be gathered within the framework of third-pillar joint supervisory authorities (e.g. the Schengen JSA) and Eurodac. The Garante took part in the drafting of the OECD Recommendation on Enforcement, which is expected to be adopted in the coming months. Reference should also be made to the contribution provided by the Italian delegation to the discussion on enforcement issues within the framework of the Case Handling Workshops held in 2005 and 2006, where a tentative Decalogue of inspection best practices was proposed and discussed.

- Has your DPA been involved in 2005-2006 in cross-border enforcement activities? If so, what has been accomplished or learned?

Yes, although cross-border enforcement cases were not many and mostly concerned SPAM and unsolicited advertising. Whilst co-operation with other DPAs was good, a point to make is that the handling timeframe in these cases was excessive by having regard to the nature of the cases addressed.

- What would be in your view priority areas for cross-border enforcement cooperation?
Especially “at risk” areas for data protection include the establishment and management of large databases and the use of new technologies.
- Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation?
No. The cases addressed so far where handled by the competent legal matters departments with the help of the community and international matters department.
- Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...)?
It is unquestionable that such practical tools facilitate international co-operation as regards enforcement; however, it might be appropriate to consider the joint development of unified methods/practices to carry out sector-related audits with particular regard to large databases and electronic communications networks.

SPAIN - national

1. Inspections and audits

Organisational aspects

- Is there a specific department in your authority dedicated to inspections or audits?

YES, the Deputy Direction of Inspection

- If possible, provide staff numbers and budget for enforcement (inspections and audits)

Deputy Direction of Inspection consists of the following human resources (all public officers)

- 19 Inspectors
- 14 Legal Experts (resolution drafters)
- 17 auxiliary staff

- How many of dedicated staff are technical experts? Legal experts? *SEE ANSWER ABOVE*
- Does the composition of that department influence the objectives and results of the inspections or audits?

The composition of the department is a consequence of the different steps that make up our inspection procedure. Both technical and legal analyses are essential parts of a same procedure and both allow the Spanish DPA to have results of inspections and audits fully comprehensive of all the aspects involved.

1. Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

It is a general trend that the inspections and audits we carry out improve in some way the spread of data protection awareness in all sectors of the society. It is therefore needed to cover as many topics and sectors of activity as possible. In that sense we could consider as highly desirable to have the capability of adapting autonomously our human resources to our needs and the function we have to develop.

Inspection policy

- Does your office have an inspection or audit policy, with annual selection of priorities and targets? If so, on what basis and how are priorities and targets determined? If not, how do you determine objects for inspection or audit?

The enforcement competences of the AEPD include reactive actions consisting in investigation of privacy violations as a consequence of a complaint or by own initiative (if we take knowledge of a violation by any other mean –media-), and preventive actions -ex officio-audits (sectorial plans, in our terminology because are referred to a certain sector).

Relating to preventive actions, the ex officio plans involve investigation of a specific sector to verify fulfilment and adapt it. The sectors are chosen annually following different criteria, being the main one an increase in the complaints received concerning that concrete activity.

The purpose is to make a series of recommendations that allow those responsible to adapt to the legislation on matters of Data Protection (these audits never end with fines).

- Do you have a publicly available planning of inspections or audits?

We have annual planning of ex officio audits but they have the consideration of an internal document

- Please illustrate choice of priority areas made recently.

The AEPD has carried out 20 sectorial audits in the seven past years. The list of sectors audited is:

2006:	<i>Public and Private Schools</i>
2005:	<i>Personnel Recruitment by Internet</i>
2004:	<i>Hospital laboratories and firms that provide them services</i> <i>National Public Administration Institute</i> <i>Hotel Chains</i>
2003:	<i>National Statistics Institute</i> <i>Censuses of Population and Housing</i>
2002:	<i>Competitions, games and television raffles</i> <i>Remote Banking (Bank on-line)</i> <i>Common file on asset insolvency</i>
2001:	<i>National Statistics Institute</i> <i>Historic File of Car Insurance</i> <i>Large Department Stores</i>
2000:	<i>Electronic Commerce</i> <i>Hospitals</i> <i>National AIDS Register</i> <i>Directorate General of Traffic</i>
1998:	<i>Bingo Halls</i>
1997:	<i>Public Hospitals</i>

*You can find all our recommendations on the following link:
<https://www.agpd.es/index.php?idSeccion=75>*

- Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice.

As mentioned above, we carry out inspections based on a complaint or by own initiative (if we take knowledge of a violation by any other mean –media-), and preventive actions -ex officio- audits (sectorial plans, in our terminology because are referred to a certain sector). Even if we don not classify the inspections themselves, the team responsible is specialised depending on the exact sector of activity being object of inspection/audit.

The enforcement tools are very broad: request of documents and data; examine these in the place where they are deposited, as well as inspect the physical and logical equipment used to process data, with access to the premises where these are installed; subpoenas, etc. As a result of an inspection the Director can order the cessation of the processing when it doesn't

comply with the provisions of the law. The AEPD inspectors have the status of a public authority to perform their duties.

The inspection methods and procedure are regulated in the LOPD, article 40, and in the Royal Decree 1332/1994 (art 18). The AEPD must attend all requests and complaints filed by the persons affected.

- Similarly, do you make a clear distinction between security audits and privacy audits, or between organisational and IT audits? Please explain your practice.

NO, we don't make such a difference

Recent experiences

- How long has there been an inspection or audit activity in your DPA? If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success?

The most recent audit (ex officio) we carried out was conducted over the 2 last years and was presented on 28 January 2007. The results of it gave rise to an ex officio sectorial plan for non-university regulated education. The origin of that plan lays in the concern expressed by the Parliament over the personal data processed by schools and high schools, specifically emphasising processing health data, even of mental health, the probable scarcity of specific measures implemented by the schools and the existence of un-notified files. Due to this, the Subdirectorate of Inspection commenced work to draw up an Ex Officio Sectorial Plan to allow it to ascertain the level of fulfilment of the laws on data protection by schools teaching non-university education. The main areas of concern detected were :

- *Information and consent to the processing of data*
- *Quality of the data during the different steps of the processing*
- *Adequate safeguards of the rights in matters of data protection(access, correction, cancellation and opposition)*
- *The level of security to be implemented, with special attention to the so called specially protected data*

Moreover, advice for minors on use of personal data was prepared and distributed at more than 14,000 schools.

- Please provide recent figures, if possible distinguishing between the different types of inspections and audits?

In 2006 the AEPD carried out 1.282 investigation procedures that finished with 281 sanctions procedures and 103 sanction procedures against public administration bodies.

- Which inspections or audits do you consider as especially noteworthy? Please describe results and lessons learned.

The inspection mentioned above on centres providing non-university regulated education has meant a significant experience both for the dimensions of the inspections (with a considerable effort in terms of technical and human resources) and for allowing the AEPD

to improve the awareness of the importance of the fulfilling of the legal protection requirements in such a an important sector.

2. Sanctions and other measures

Organisational aspects

- Is there a specific department in your authority responsible for sanctions and other measures?

The Department of Inspection is also in charge for the proposal of sanctions that have to be agreed jointly with the Director of the Spanish DPA.

- If possible, provide staff numbers, professional experience and workload. *SEE ANSWER TO QUESTION 1*
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

We have very broad enforcement competences (investigative, subpoenas, checking in situ, imposing fines, etc) what is essential to provide a factual protection to citizens. However, we could consider as a barrier the legal obligation to attend and resolve any single complaint submitted to us, well founded or not, what can be an obstacle to develop investigative work (limited human resources can not attend properly such a huge number of complaints).

Recent practice

- Please provide for recent figures for different types of sanctions and other measures available to your authority?

Following the Spanish Data Protection Law (art. 45), the sanctions that can be imposed by the AEPD vary depending on the type of infraction committed:

Minor infringements: 601- 60.101 €

Serious infringements: 60.101-300.000 €

Very serious infringements: 300.506- 601.000 €

Regarding the amount of the sanctions, for instance, the highest one related with the remittance of mail with advertising unsolicited was of 540.000 € (in 2006). Concerning SPAM the highest sanction was of 150.000 € (in 2005). We have also had a recent case where we imposed a sanction for the use of “peer to peer” software (exchange of music, videos..): the software was installed in a PC at the workplace allowing as a consequence the access to files with personal data related to workers.(6.000 € sanction)

- Which sanctions or measures not yet available to you would be useful?

One of the areas we are not competent on is the supervision on freedom of information or to provide prior checking assessment in files with a specific risk. We would consider useful to have these tools between our enforcement powers.

- Are decisions on sanctions or other measures systematically made public, and if so, how? If not systematically, on what grounds does your DPA make the decision to give the cases publicity?

YES. In 2004 the AEPD issued an Instruction (1/2004) on the disclosure of its resolutions) where it is established that, once the decision has been communicated to those parts interested in the procedure, has to be made public in the month that follows the notification. The publication is made through our website: www.agpd.es

- Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof.

The sanctions are part of our role to make society aware of the importance to fulfil the legal obligations in terms of data protection. Some of the sanctions we have imposed dealt with activities the citizens are well involved with (like the one on “peer to peer” software) so we consider it is also an important way to develop our role. Moreover, the press plays an important role in this aspect, being our most relevant decisions communicated to them via press releases.

- Which actions do you consider as especially noteworthy? Please describe results and lessons learned.

The AEPD launches mass communication activities in order make data controllers aware of the data protection obligations. Examples of these activities are the presentation of the new simplified on-line file notification system called “NOTA” (July 2006), the First European Congress on Data Protection (march 2006), courses and seminars for data controllers, divulgation conferences and sessions and communication in co-operation with the Chambers of Commerce of Spain. All of them has allowed us to up to date our daily activity to the concrete needs pointed out by the different sectors.

3. International cooperation for enforcement

The OECD report contains very useful information on that subject and concludes with a number of possible topics for further study. We would like you to consider the following questions, inspired to a large extent by the OECD report:

- Has your DPA been involved in 2005-2006 in cross-border enforcement activities? If so, what has been accomplished or learned?

Yes, the AEPD has cooperated actively with other European DPAs based on article 28.6 of the Directive 95/46/CE, especially on spam violations.

Out from the EU scope, in the exercise of the competence set up in article 37.1 of the LOPD (...to perform the functions of international co-operation in matters of personal data protection), we have signed a Memorandum of Understanding with the Federal Trade Commission of the US, for cooperation in the fight against spam violations.

Due to the similar enforcement abilities of the FTC and AEPD (ability of subpoenas, request of information, checking in situ, cessation of processing, etc) we are able to mutual assistance and cooperation, especially after the US CAN Spam ACT that reinforce the competences of the FTC in the field of privacy in telecommunications.

The AEPD is also part of the Spanish Delegation of the OECD Working Party on Information Security and Privacy(WPISP).

- What would be in your view priority areas for cross-border enforcement cooperation?

AEPD believes that we should reflect on what we can do with the current legal instruments we have (at OECD level, at EU level and Council of Europe level, Asia-Pacific Level, national laws, etc) and what we need if this is not enough. We should improve international enforcement cooperation among all authorities and public bodies that have the task of defending citizens privacy rights since the future of the “privacy or data protection” will depend on the credibility of the Supervisory Authorities in providing an effective protection against violations.

- Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation?

Apart from the concrete request for cooperation by other colleagues, the AEPD is an active member (as part of the Spanish delegation) of the OECD Working Party on Information Security and Privacy (WPISP).

- Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...) ?

We should consider the possibility for the Supervision Authorities to help each other in the compliance of the administrative sanctions as well as provide the inspectors with access to documents and files object of investigation.

SPAIN - Catalonia

1. Inspections and audits

Organisational aspects

- Is there a specific department in your authority dedicated to inspections or audits? *Yes, but the same department is dedicated for inspections and sanctions.*
- If possible, provide staff numbers and budget for enforcement (inspections and audits) *7 people*
- How many of dedicated staff are technical experts? *3 people Legal experts? 4 experts*
- Does the composition of that department influence the objectives and results of the inspections or audits? *no*
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives? *We need that the technical experts were civil servants, too.*

Inspection policy

- Does your office have an inspection or audit policy, with annual selection of priorities and targets? *Yes, but we also make inspections related to the complaints that we receive* If so, on what basis and how are priorities and targets determined? *According to the complaints that the Inspection Area receives, we decide our priorities and targets* If not, how do you determine objects for inspection or audit?
- Do you have a publicly available planning of inspections or audits? *No*
- Please illustrate choice of priority areas made recently. *Public Security and Public Health Areas*
- Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice. *We don't classify inspections according these criteria, we make inspections based on the complaints made by citizens and the determined targets*
- Similarly, do you make a clear distinction between security audits and privacy audits, or between organisational and IT audits? Please explain your practice. *The staff of the Inspection Area is composed by legal experts and technical people, so depending on the audit, we organize the inspections team*

Recent experiences

- How long has there been an inspection or audit activity in your DPA? Since two years ago If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success? *Provide us with special technological equipment, special formation for the inspectors, exchange of experiences with other DPA...*

Key-factors: To create an standard form of inspection's act, to lay down a list of best practice, to define the purpose and goals of the specific act of inspection and an accurate previous preparatory work.

- Please provide recent figures, if possible distinguishing between the different types of inspections and audits? *Technical inspections, legal inspections and mixed inspections*
- Which inspections or audits do you consider as especially noteworthy? *We made some inspections in Barcelona's Hospitals in order to verify the access to the medical files with a non medical purpose Please describe results and lessons learned. We detect the*

infraction of the Spanish data protections law. Since we had to do several inspections about the same issue, then we could improve the whole inspection act.

2. Sanctions and other measures

Organisational aspects

- Is there a specific department in your authority responsible for sanctions and other measures? *No, is the same than the Inspections Area*
- If possible, provide staff numbers, professional experience and workload. *4 people*
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives? *Yes*

Recent practice

- Please provide for recent figures for different types of sanctions and other measures available to your authority? *Our sanctions always consist in a requirement that suppose to stop the processing of data, or to process the data in proper conditions (technical, organizational...)*
- Which sanctions or measures not yet available to you would be useful? *Economical sanctions (fines)*
- Are decisions on sanctions or other measures systematically made public, and if so, how? *No* If not systematically, on what grounds does your DPA make the decision to give the cases publicity? *In the Annual Report we explain anonymously the main inspections and sanctions in general terms*
- Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof. *We have detected that once we request information about the complaint there is a change of attitude in the requested organization. They begin to improve their observance of the law. To be in touch with the DPA raises awareness of data protection law.*
- Which actions do you consider as especially noteworthy? Please describe results and lessons learned. *We adopted a preventive measure against the file of the police and the organization made all our requested changes in order to make us to cancel the measure*

3. International cooperation for enforcement

The OECD report contains very useful information on that subject and concludes with a number of possible topics for further study. We would like you to consider the following questions, inspired to a large extent by the OECD report:

- Has your DPA been involved in 2005-2006 in cross-border enforcement activities? *No* If so, what has been accomplished or learned?
- What would be in your view priority areas for cross-border enforcement cooperation?
- Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation?
- Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...)?

SPAIN - Madrid

1. Inspections and audits

Organisational aspects

- Is there a specific department in your authority dedicated to inspections or audits?
Yes
- If possible, provide staff numbers and budget for enforcement (inspections and audits)
Head of the Department + 3 Full Time Inspectors + 1 Full Time Administrative Assistant + 2 Part Time Computer Experts. There is no specific breakdown for the inspection department or audits. The needed resources are taken from the general budget on items like salaries, expenses, computer equipment, etc.
- How many of dedicated staff are technical experts? Legal experts?
The three inspectors are legal experts. The technical support in the audits is provided by persons (2) working in the IT Department.
- Does the composition of that department influence the objectives and results of the inspections or audits?
The composition of an administrative department always influences its goals and results but although the possibility of improving the situation is present at any time (i.e. a Full Time IT Expert would be welcomed) we are rather satisfied with the resources we have at this moment.
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?
The qualifications of the staff are excellent and perfectly suited for the tasks they carry out. For other comments, see the previous point.

Inspection policy

- Does your office have an inspection or audit policy, with annual selection of priorities and targets? If so, on what basis and how are priorities and targets determined? If not, how do you determine objects for inspection or audit?
Yes. There is a yearly planning and in this planning priorities are defined. For instance, this year, we are focusing on the implementation of the mandatory policy for security audits in the Local Administration and in the inspection of the processing of personal data in the Social Services both at the regional and local level.
- Do you have a publicly available planning of inspections or audits?
Every December, the planning for all the activities of the Madrid DPA is established and all them are planned and scheduled. This comprises the raising awareness, training, registry, consultancy, enforcement, inspection and audit actions. The Annual Planning is sent to all the Public Bodies under the supervision of the Madrid DPA for them to know what actions of the DPA are affecting them during the whole year.
Besides, in the area of the Inspection Department, a big share of the available time is consumed by dealing with the complaints lodged by citizens. This aspect of the work it is not easily subject to planning but, in general, based on statistics from previous years, we try to make up our minds about the expected workload we will have in the next year.
- Please illustrate choice of priority areas made recently.
As explained above, we have started last year a systematic approach to encourage data controllers to comply with their obligations to carry out a security audit every two years. Last year we began with the Regional

Administration and in 2007 we are focusing in the Local Administration. Besides, we have defined and begun to apply a yearly procedure to assure compliance with this requirement by all data controllers under our supervision. It was also decided that the other priority for the year would be to check compliance with data protection legislation in the Social Services field. The main reasons for the decision was that we receive many request for advice in this field and because of the sensitivity of the information processed in this area and, last but no least, we would like to check the degree of implementation of a Recommendation produced by the Madrid DPA in this area in the year 2004.

- Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice.

Three different categories of inspections can be outlined.

- 1. Complaints based inspections: After a complaint has been lodged, there are some facts that need to be checked. These inspections are very specific and focused on the file(s) or database(s) involved in the complaint and not only because of operational reasons but also because of the case law in Spain does not allow “fishing expeditions” when investigating a complaint. So that, these inspections only try to clarify the relevant facts in the case under scrutiny.*
- 2. Ex officio inspections: There are two situations in which this kind of inspection is carried out. In the first one, the DPA gets to know by different means (namely, news on the media) that a specific public body may not be complying with the data protection regulations when processing personal data. The second one happens if after continued work by the Consultancy Department in a specific area, the data controller(s) fail(s) to follow the advice for different reasons. In both cases, enforcement actions from the Data Inspection Department are launched (for instance, in the last year two broad enforcement actions were launched involving city councils that after years of contacts and guidance from the Consultancy Department have not notified their personal data processing operations and public controllers obliged to perform a security audit that have not reacted to the requirements of the Madrid DPA)*
- 3. Sector Inspection Plans (which are ex officio too): These are proactive inspections without a sanctioning aim and that are defined in the data protection legislation of the Region of Madrid to check a whole sector of the Regional or Local Public Administration in order to find out the weaknesses, shortcomings or low compliance areas and, afterwards, to issue the relevant adequacy instructions. These instructions are binding and are made public. This kind of audits review all the aspects an organisation must take into account and implement for complying with data protection legislation and could be qualified as “full-fledged audit”.*

- Similarly, do you make a clear distinction between security audits and privacy audits, or between organisational and IT audits? Please explain your practice.

In general terms, it cannot be said that we made distinctions between security audits and privacy audits. For us security is only a part of the requirements for establishing a good data protection policy and practice. Security issues are checked jointly with all the other

principles in sector audits and, of course, when we receive a complaint that focuses in the lack of adequate security measures.

Nevertheless, as already explained in a previous point (Inspection Policy), we have started a yearly procedure to request the biennial security audits report to the affected data controllers (those having personal data files considered as needing medium or high security measures according to the Spanish regulation in the matter).

Recent experiences

- How long has there been an inspection or audit activity in your DPA? If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success?

In the Madrid DPA the inspection activity has been in place for several years but mainly focused in the individual cases. In the past years, a new trend has also developed: The enforcement actions by the Data Inspection are used with controllers that refuse or fail to comply with the advice and guidance from the DPA and, thus, it is a useful tool to show them that after many opportunities for voluntary compliance, stronger actions may come.

At this moment, it may be useful to make a historical introduction. In the beginning of the activities of the Madrid DPA (1997), a strong focus was put on the training, education and raising awareness activities and there was not a separated Inspection Department: The inspections and consultancy areas co-existed within a single department. After some years of functioning, it was felt that a progressive shift in the focus was needed and more separation of roles was implemented until, finally, in 2004, two separate departments were created: Registry and Consultancy in one hand and Inspection and Control in the other, whose heads report directly to the Director of the Agency and are members of the steering committee of the DPA. Under this scheme, both Departments work together and exchange information but the data protection consultants preserve the confidentiality of the failures or shortcomings present in the data controller processing operations that they may know because of their consultancy work unless there is no cooperation or reaction to the advice and, at the same time, the inspection keeps confidential the details of the enforcement actions in place (only general information on a specific controller being under investigation is forwarded to the Consultancy Department).

This ongoing process meant an important cultural and organisational change, that has not ended yet, as we have working in the last year in a further step forward in the direction of stressing enforcement actions, (as already explained) in a more general approach by implementing the Sector Inspection Plans. This new reality needs a cultural change and the management of this change namely because of the special configuration of our office that works very closely with data controllers helping them to comply with the law. This is the main task of the Consultancy and Registry Department. Therefore, it may happen that in a Sector Inspection Plan a body be chosen for auditing because it is greatly representative of the sector under scrutiny and, at the same time, there is ongoing consultancy work being carried out in the same organisation. In that case, a very good coordination and team work with the Consultancy Department is crucial for achieving good results and forwarding to the data controller the right information and the reasons and goals of the inspection. To a lesser degree, this is also true even though there is no direct work at the moment in the bodies chosen for inspection.

- Please provide recent figures, if possible distinguishing between the different types of inspections and audits?

In 2006, 92 inspections can be qualified as ex-officio actions, whilst 77 were complaint based.

- Which inspections or audits do you consider as especially noteworthy? Please describe results and lessons learned.

We already mention two important enforcement actions. The first one affected to 13 city councils that have not notified files. After the enforcement action was started, there were 11 that notified the files whilst two of them got a decision establishing they have failed to comply with the law and it was forwarded to the Ombudsman. Afterwards, both of them were working with the Agency to regularize the situation.

The other one affected to the data controllers that have not reacted to the request from the Consultancy Department to forward to the DPA the security audit reports. 47 inspections were started and, within three months, we received 45 reports.

The lesson learned is that a progressive and practical approach to compliance, starting with the provision of information and guidance followed by formal requests and, for those not reacting to the voluntary approach, applying enforcement actions produces very good and timely results.

2. Sanctions and other measures

Organisational aspects

- Is there a specific department in your authority responsible for sanctions and other measures?

Yes. The Data Inspection Department.

- If possible, provide staff numbers, professional experience and workload.

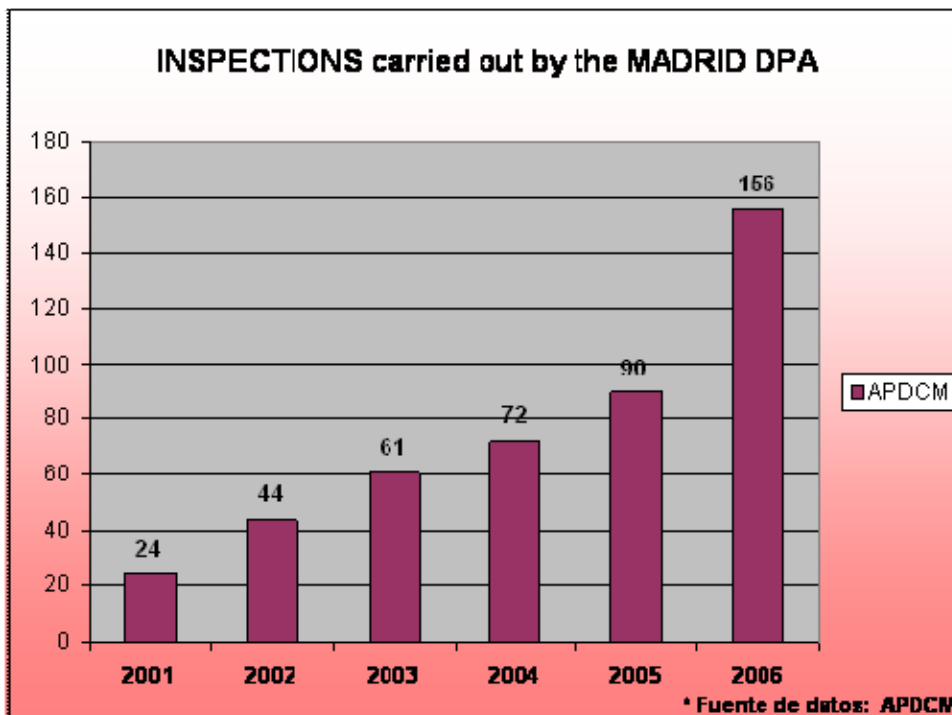
The Head of the Department, 3 inspectors (legal experts), 1 Administrative Assistant and 2 Part Time IT experts. In the last year, the Department dealt with 169 cases (13 of them were complaints because of the refusal of granting the rights of access, rectification, deletion or to object, that must follow a special proceeding according to the Spanish law).

- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

See Point 1

Recent practice

- Please provide for recent figures for different types of sanctions and other measures available to your authority?



It does not contain information on the special proceeding dealing with the refusal of rights (13 cases in 2006).

- Which sanctions or measures not yet available to you would be useful?
We do not feel extra powers or measures are needed
- Are decisions on sanctions or other measures systematically made public, and if so, how? If not systematically, on what grounds does your DPA make the decision to give the cases publicity?
Until very recently, most of the decisions on the cases were published by the Madrid DPA through different channels, like the digital review datospersonales.org, that has already published 25 issues and has 7.000 subscribers, or the information included in the annual reports. But, for increased transparency of our activities and for providing better information to the public, it has been decided very recently to systematically publish all the decisions (suppressing any kind of personal data) on inspection cases (ex officio or complaint driven). The publication will be carried out through our institutional website 45 days after the decision is taken (the parties can ask the Director of the DPA to reconsider his or her decision within one month, the other 15 days provide for a security cushion for notification of the decisions to the parties). Besides, since November 2006, the decision of one relevant case is always highlighted in the home page of our website.
- Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof.
In the field in which we work, the mere declaration that a Public manager has not complied with the provisions of the Data Protection Act is quite effective. Besides, now we publish all the decisions in our website and the most relevant ones find their way to the media in a very short time even though we do not communicate them to the press.

And last but not least, all the sanctioning decisions are forwarded to the Ombudsman, who includes the detected infringement in the annual report of the institution.

- Which actions do you consider as especially noteworthy? Please describe results and lessons learned.

In our experience, the mere launching of an investigation procedure by the Data Inspection regarding a specific public body has a considerable effect in the affected institution (it is even bigger if you take into account the Madrid DPA invest a lot of time and effort in training and raising awareness among data controllers with members of the office working directly with them to encourage compliance) as it is seen as a shift in the normal pattern of relationship with the DPA. This effect is even stronger if it ends with an infraction declaration that now is published and, in many cases -as the decision is also communicated to the complainant- it normally appears in the media.

3. International cooperation for enforcement

The OECD report contains very useful information on that subject and concludes with a number of possible topics for further study. We would like you to consider the following questions, inspired to a large extent by the OECD report:

- Has your DPA been involved in 2005-2006 in cross-border enforcement activities? If so, what has been accomplished or learned?

No

- What would be in your view priority areas for cross-border enforcement cooperation?

This is more a matter for the Spanish Data Protection Agency as given the scope of our competence it is would be not very usual we should have to enter into cross-border enforcement activities.

Anyway, and although it is not a cross-border activity, there is a frequent and fruitful cooperation with the Spanish Data Protection Agency in those cases in which the competences of both authorities must be exercised.

- Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation?

No

- Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...)?

For the cross-border cooperation in the enforcement field to be successful is crucial to define common standard for each party clearly know what could be expected from the actions of other DPAs invo

SWEDEN

1. Inspections and audits

Organisational aspects

Q Is there a specific department in your authority dedicated to inspections or audits?

A *Since April last year the Data Inspection Board has a new organisation and now there are three operative teams all dedicated to inspections and audits. The teams are responsible for certain sectors; team on medical care, research and education, team on industry, team on public authorities and working life. Then there is one team on information and service.*

Q If possible, provide staff numbers and budget for enforcement (inspections and audits)

A *The three operative teams have 7 or 8 persons each. The total budget for the Data Inspection Board is fully 31 million SEK. A budget for inspections and audits is not available.*

Q How many of dedicated staff are technical experts? Legal experts?

A *There are 3 technical experts and 24 legal experts.*

Q Does the composition of that department influence the objectives and results of the inspections or audits?

A *We are not quite sure of what you mean by this question. However, we will make a few comments under this point. First we would like to point out that our definition of “audit” is wider than “inspection”. An audit can be both a written procedure, a questionnaire and a field inspection whereas an inspection is normally a field inspection. When we carry out a field inspection there are normally two lawyers and one IT-expert participating.*

Q Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

A *We have a budget limit and we have to adapt the audit objectives to this limit. We do not think that the budget limit is sufficient for the tasks that the Data Inspection Board has been assigned and therefore we have requested a 10 % increase of our budget.*

Inspection policy

Q Does your office have an inspection or audit policy, with annual selection of priorities and targets? If so, on what basis and how are priorities and targets determined? If not, how do you determine objects for inspection or audit?

A *Yes. We have an audit policy (including both audits and inspections) as well as an audit plan (planned in advance). The audit policy lays down criteria for selection of when we shall initiate an audit. The audit plan lays down what data controllers that shall be subject to an audit or inspection. Then there are also audits that the general public brings to the authority. We give priority to objects where we have to make follow-up audits and to sectors regarding which we receive many complaints. The Data Inspection Board also gives priority to objects regarding new technology and new systems which we have a duty to observe and describe. We always give priority to cases where sensitive data are at stake.*

Q Do you have a publicly available planning of inspections or audits?

A *No, it is not publicly available.*

Q Please illustrate choice of priority areas made recently.

A *e-Government, inventory of databases held by police authorities, electronic footprints (e.g. the use of electronic keys in apartment blocks and the use of electronic tickets in public transport), the use of personal data in schools, pharmacies' use of electronic prescriptions.*

Q Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice.

A *Yes. We have fact-finding audits regarding new phenomena where we have no or little experience, audits based on complaints, audits on a specific file (occurring rather frequently and planned in advance). As to "fully-fledged" audits we are not quite sure of what you mean. If you by fully-fledged mean an inspection covering all data processed by a data controller then the answer is that we sometimes carry out this kind of audit. If, on the other hand you by fully-fledged mean an audit covering a whole sector in society the answer is that we carry out such audits yearly. We call them "field inspections". The latest one took place this past autumn and referred to the sector of private insurance companies. In case we want to carry out an audit regarding a whole sector we also make use of questionnaires.*

Q Similarly, do you make a clear distinction between security audits and privacy audits or between organisational and IT audits? Please explain your practice.

A *Yes, we make such a distinction. The most common audits are privacy audits. As regards sensitive data the privacy audit is complemented by a security audit. These two audits are carried out at the same time by different categories of staff.*

Recent experiences

Q How long has there been an inspection or audit activity in your DPA? If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success?

A *Since 1973 when the Data Inspection Board was established.*

Q Please provide recent figures, if possible distinguishing between the different types of inspections and audits?

A *Audits carried out in 2006 according to the Personal Data Act (1998:204) amount to 147 (of which 52 were field inspections, 10 questionnaires and 85 written procedures). Apart from these audits we also carried out audits according to the Credit Information Act and the Debt Recovery Act.*

Q Which inspections or audits do you consider as especially noteworthy? Please describe results and lessons learned.

A *We will have to answer this question later.*

2. Sanctions and other measures

Organisational aspects

Q Is there a specific department in your authority responsible for sanctions and other measures?

A *No*

Q If possible, provide staff numbers, professional experience and workload.

A *Not applicable*

Q Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

A *Please see the answer to the corresponding question under 1. Inspections and audits – Organisational aspects, the last question*

Please find below an explanation to the answers.

According to the Personal Data Act, the Data Inspection Board is entitled, for its inspections and audits, to obtain on request a) access to personal data that is processed, b) information and documentation of the processing of personal data and security of this processing, and c) access to the premises linked to the processing of personal data. Furthermore, if the Board cannot obtain sufficient information in order to conclude that the processing of personal data is lawful, it may prohibit the data controller to process data in any other manner than by storing them. This prohibition may be subjected to a default fine. The same thing is valid if the Board concludes that the processing is unlawful. A default fine may also be prescribed if the controller does not voluntarily comply with the Board's decision on security measures. The Board may also apply to the County Administrative Court for erasure of such personal data that has been processed in an unlawful manner.

Recent practice

Q Please provide for recent figures for different types of sanctions and other measures available to your authority.

A *Not applicable*

Q Which sanctions or measures not yet available to you would be useful?

A *No opinion*

Q Are decisions on sanctions or other measures systematically made public, and if so, how? If not systematically, on what grounds does your DPA make the decision to give the cases publicity?

A *Decisions regarding deficiencies according to the Personal Data Act are sometimes made public and made available on our website. Our aim is to publish 4 or 5 press releases per month, since we believe that this is the most efficient way to reach the data controllers and the general public with our message.*

Q Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof.

A *We believe that making a decision public sometimes can be very effective. We both disseminate our opinion on how to apply the legislation on data protection and put pressure on the data controller.*

Q Which actions do you consider as especially noteworthy? Please describe results and lessons learned.

A *As to actions that ought to be mentioned we always try to make the data controller who has breached a data protection rule to rectify himself by calling attention to the deficiency. The data controller has to undertake to make a rectification and not until this has been accomplished we close the case. If, on the other hand the data controller does not rectify*

himself the Data Inspection Board has other possibilities to act. The powers of the Data Inspection Board are described under 2. Sanctions and other measures – Organisational aspects, the last question.

We have also worked out a flowchart to be applied when handling a case. At present it is only available in Swedish but we will have it translated into English.

3. International cooperation for enforcement

Q Has your DPA been involved in 2005-2006 in cross-border enforcement activities? If so, what has been accomplished or learned?

A Yes, the Data Inspection Board has participated in the ETF (the Enforcement Task Force) regarding private insurance companies' processing of personal data. We have not yet received the overview of the results, so we will have to comment on this later.

Q What would be in your view priority areas for cross-border enforcement cooperation?

A We need to discuss this further.

Q Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation?

A No, such cooperation has to be handled within the time- and budgetary frame given.

Q Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...)?

A First of all we would like to draw conclusions from the cross-border activity in which we have participated already, that is the ETF (see above). At present we see no need for a common activity, but of course it is a good thing to have a framework for handling cases that concern all the DPAs.

SWITZERLAND

1. Inspections and audits

Organisational aspects

- Is there a specific department in your authority dedicated to inspections or audits?
No, we have 2 departments for data protection. Each department is responsible for advices and inspections. For technical audits, we have also a competence's centre with IT-experts.
- If possible, provide staff numbers and budget for enforcement (inspections and audits)
We don't have specific staff and budget for enforcement.
- How many of dedicated staff are technical experts? Legal experts?
4.7 = technical experts (Informatic); 7.7 legal experts
- Does the composition of that department influence the objectives and results of the inspections or audits?
No
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?
No

Inspection policy

Remark: We think it would be important to define what we mean with inspection and what we mean with audit.

- Does your office have an inspection or audit policy, with annual selection of priorities and targets? If so, on what basis and how are priorities and targets determined? If not, how do you determine objects for inspection or audit?
We have defined intervention's criteria: sensitivity of the data, number of the persons concerned, insider's information, position of the individual (for example relation of subordination), interpretation of legal rules or data protection principles, public interest, etc. We define also some annual priorities or targets
- Do you have a publicly available planning of inspections or audits?
Not actually
- Please illustrate choice of priority areas made recently.
Video surveillance of employees in a Cinema
Video surveillance in a hypermarket
Drug test in a Railway company
Processing of inaccurate Data in a credit information company
- Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice.
We can distinguish between inspection based on complaints or informations we received from insiders, media or other sources. We also planned inspection on basis of observations we are making (for example FAQ).

- Similarly, do you make a clear distinction between security audits and privacy audits, or between organisational and IT audits? Please explain your practice.

No actually we don't make a clear distinction. But generally our inspections are focusing principally on privacy aspects. We define for all inspections which points we will examine. Depending of the subject, we will examine more technical aspects or more legal aspects.

Recent experiences

- How long has there been an inspection or audit activity in your DPA? If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success? *We have just finished with an inspection video surveillance in a supermarket (see attachment). It is important to investigate seriously a case, in particular to request the production of all relevant informations and documents, to have contact with the data controller, his staff and all relevant involved persons, to inspect on the spot. It is also important to make realistic and practicable proposals of corrections or improvements. It is also important to indicate clearly to the data controller the scope of the investigation, the legal environment and the possible "sanctions". The possibility to inform the public of the results of our investigations is also a factor for success.*

- Please provide recent figures, if possible distinguishing between the different types of inspections and audits?

- Which inspections or audits do you consider as especially noteworthy? Please describe results and lessons learned.

We think it is important to have a positive approach of an inspection. Our objective is not necessary to sanction, but to verify if a data processing is respecting data protection regulations and to propose corrections or improvements. It is important to maintain a cooperative approach with the data controller and to sanction when there are no other possibilities to obtain corrections or improvements.

2. Sanctions and other measures

Organisational aspects

- Is there a specific department in your authority responsible for sanctions and other measures? *No, we don't have the possibility to sanction. We can address recommendations to the data controller.*
- If possible, provide staff numbers, professional experience and workload.
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

NO

Recent practice

- Please provide for recent figures for different types of sanctions and other measures available to your authority?
- Which sanctions or measures not yet available to you would be useful? *Fees or penal sanction*
- Are decisions on sanctions or other measures systematically made public, and if so, how? If not systematically, on what grounds does your DPA make the decision to give the cases publicity?

We normally publish all our recommendations. If there is a public interest, we publish the recommendation with the name of the data controller.

- Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof.

In some situations mainly in the private sector is the publicity quite effective. We would like to have also (like others colleagues in Europe) the possibility of fees and sanctions which we consider effective

- Which actions do you consider as especially noteworthy? Please describe results and lessons learned.

Publicity about a measure

3. International cooperation for enforcement

The OECD report contains very useful information on that subject and concludes with a number of possible topics for further study. We would like you to consider the following questions, inspired to a large extent by the OECD report:

- Has your DPA been involved in 2005-2006 in cross-border enforcement activities? If so, what has been accomplished or learned? *no*
- What would be in your view priority areas for cross-border enforcement cooperation? *Credit Information; health; insurance; law enforcement; Off shore; CRM, personal data files; ...*
- Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation? *Not specially (a part from the participation to the JSA-Schengen + Eurodac)*
- Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...) ? *yes*

UNITED KINGDOM

1. Inspections and audits

Organisational aspects

- Is there a specific department in your authority dedicated to inspections or audits?
The Information Commissioner's Office (ICO) has an Audit Team based within the Regulatory Action Division (RAD).
- If possible, provide staff numbers and budget for enforcement (inspections and audits)
The team currently consists of 3 staff. A second team of 2 staff is under active consideration and is likely to be operational this year.
- How many of dedicated staff are technical experts? Legal experts?
The current team are predominantly legal (compliance) experts although there is a level of IT knowledge within the team. A plan for bringing in additional technical expertise for specific audits is being developed.
In the past Compliance Team members have also been co-opted on to audits where they have specific sectoral experience and this is an idea which may be employed again in the future.
- Does the composition of that department influence the objectives and results of the inspections or audits?
Yes - in as much as we do not have the technical capability to 'test' assurances / responses to technical questions but unless there are evidenced issues relating to the technical capability it is unlikely to have a significant impact on conclusions etc.
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?
Yes but potentially we have the flexibility to shape the team in line with objectives.

Inspection policy

- Does your office have an inspection or audit policy, with annual selection of priorities and targets? If so, on what basis and how are priorities and targets determined? If not, how do you determine objects for inspection or audit?
Inspection is covered by the (RAD) strategy. The programme will be a mixture of a targeted sector or specific type of processing (e.g. data sharing, data controllers where there have been identified compliance issues, as checks on formal undertakings and requests from data controllers.

Sector / Processing targets are likely to be set in conjunction with the Deputy Information Commissioner and focus on areas where the processing can have significant impacts on individuals, where there has been or is likely to be significant changes in the nature of the processing, areas of public interest etc.
- Do you have a publicly available planning of inspections or audits?
No.
- Please illustrate choice of priority areas made recently.
Health and local authorities.
- Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice.

We can identify the background to the audit (see a. above) but the approach would generally be the same a fully fledged audit although the scope will obviously vary.

- Similarly, do you make a clear distinction between security audits and privacy audits, or between organisational and IT audits? Please explain your practice.

The majority of audits would include security, privacy, organisational and IT considerations the exception being the audits undertaken as a result of formal undertakings in which case the scope would be more specific e.g. security.

Recent experiences

- How long has there been an inspection or audit activity in your DPA? If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success?

There has been audit activity for approx 3 years.

From an organisational perspective the key considerations have been:

the mix of the team not only considering legal and technical but also sectoral knowledge and audit / analytical ability;

programme management; and

communication links with other parts of the Regulatory Organisation.

From the cultural perspective the key considerations are:

taking a more proactive rather than reactive approach; and

face-to-face interaction with data controllers.

- Please provide recent figures, if possible distinguishing between the different types of inspections and audits?

Something of the order of 17 audits has been conducted since the programme started of which 8 have been conducted in the last year. These have included an adequacy review of organisational policies and procedures followed by a compliance on-site review (normally 2/3 days) interviewing staff and inspecting records.

- Which inspections or audits do you consider as especially noteworthy? Please describe results and lessons learned.

It would be difficult to differentiate as all the audits have identified some common issues but have their own peculiarities.

A recent audit however is worthy of mention because although the data controller had a relatively poor reputation it was discovered that there was a number of initiatives underway which were positively contributing to compliance.

The key lessons would be:

never underestimate what you might find;

audits provide opportunities for identifying good practice which can be promoted across organisations; and

organisations are constantly changing and new challenges being identified in terms of how data is processed.

2. Sanctions and other measures

Organisational aspects

- Is there a specific department in your authority responsible for sanctions and other measures?

Investigations and Enforcement Teams within RAD take primary responsibility for sanctions and they are supported to a level by the Remedies team which is also part of RAD and the Legal Department.

- If possible, provide staff numbers, professional experience and workload.
*The investigations Team - 1 Head of Investigations, 7 investigators.
The Head of Investigations and five investigators are retired police officers. Of the remaining two, one is a retired Army Military Police Officer and the other is an ex-Customs and Excise Officer.*
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?
The resources and qualifications of the staff are satisfactory for the current demands.

Recent practice

- Please provide for recent figures for different types of sanctions and other measures available to your authority?
Sanctions include criminal prosecutions for unlawful obtaining of personal data. Issuing of enforcement notices and information notice may lead to criminal prosecutions for failure to comply with the notices.

During the past year the ICO issued six enforcement notices: one under the DPA - B4usearch.com; and five under the PECR - Bowater Home Improvements Limited, Bowater Windows Limited, IDT Direct Limited, Staybrite Windows Limited, Zenith Windows Limited.

Attached is a table showing criminal prosecutions during the past year.

- Which sanctions or measures not yet available to you would be useful?
There is an argument that there should be a further sanction under the Act to issue a monetary penalty to data controllers who fail to conform with their responsibilities under the Act. Where a data controller continually fails to adhere to his/her responsibilities under the Act in a manner in which harm and distress is caused to data subjects there is an argument for an immediate penalty or fast track action to a court to impose a sanction to remedy the situation quickly.
- Are decisions on sanctions or other measures systematically made public, and if so, how? If not systematically, on what grounds does your DPA make the decision to give the cases publicity?
All the above have been placed on the ICO website and have been subject of press releases.
- Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof.
- Which actions do you consider as especially noteworthy? Please describe results and lessons learned.

3. International cooperation for enforcement

The OECD report contains very useful information on that subject and concludes with a number of possible topics for further study. We would like you to consider the following questions, inspired to a large extent by the OECD report:

- Has your DPA been involved in 2005-2006 in cross-border enforcement activities? If so, what has been accomplished or learned?

The ICO has not been involved in cross border enforcement activities during 2005-2006.

- What would be in your view priority areas for cross-border enforcement co-operation?

It would be our view that cross border enforcement activity should be encouraged and that protocols should be agreed for this purpose.

- Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation?

At the current time we do not provide specific time and resources for cross border enforcement co-operation.

- Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...) ?

We are of the view that practical tools should be developed.

It should be noted that within the UK we have intelligence which suggests that those involved in unlawfully obtaining personal information are moving operations into other European states to avoid detection in the UK. This is in part due to the increased activity and success of the ICO investigations unit.

Therefore it is likely that in the future there will be a greater need to share information between Member States.

EDPS

1. Inspections and audits

Organisational aspects

- Is there a specific department in your authority dedicated to inspections or audits?

Not for the moment, although a working group of 4 has been set up to launch the inspections and audits.

- If possible, provide staff numbers and budget for enforcement (inspections and audits)

Not applicable

- How many of dedicated staff are technical experts? Legal experts?
- Does the composition of that department influence the objectives and results of the inspections or audits?
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

Inspection policy

- Does your office have an inspection or audit policy, with annual selection of priorities and targets? If so, on what basis and how are priorities and targets determined? If not, how do you determine objects for inspection or audit?

The inspection policy is currently in the making. Targets will be identified on the basis of the work done in the supervision unit of the EDPS. Priority areas are selected (see below) and will be followed up.

On top of that, the EDPS is the supervisor of the EU part of large-scale IT systems such as Eurodac and the CIS. Regular inspections and audits are taking places in these sectors as well.

- Do you have a publicly available planning of inspections or audits?
- Please illustrate choice of priority areas made recently.

The inspection this year will be conducted in the framework of the “Spring 2007” priority, the objective of which is to promote compliance of EU institutions and bodies with their obligations in terms of notifications of data processing. In frame of prior checking work certain areas have been considered as priority areas (disciplinary, medical, evaluation). These areas will also be the basis (although not solely) in inspection work.

Another area where inspections are taking place is the Central Unit of Eurodac, which the EDPS is the supervisor of.

- Do you classify your inspections according to different categories (fact-finding visit, inspection based on complaint, on a specific file, full-fledged audit)? Please explain your practice.

Different types of audits have already taken place: inspections based on a complaint, fact-finding visits, full-fledged security audit. In practice, they are treated differently, but this is still case bound and not completely systematised.

- Similarly, do you make a clear distinction between security audits and privacy audits, or between organisational and IT audits? Please explain your practice.

Recent experiences

- How long has there been an inspection or audit activity in your DPA? If it is recent (2-3 years), please explain organisational and cultural changes needed, and what you consider key-factors for success?

Institution in office only since 2-3 years. Cultural change is not really needed, since the inspection and enforcement policies are developed in parallel with the rest of the activities of the EDPS.

- Please provide recent figures, if possible distinguishing between the different types of inspections and audits? *In 2006:*
Inspections based on complaint: 2
Fact finding visits: about 6
Full security audit: 1
- Which inspections or audits do you consider as especially noteworthy? Please describe results and lessons learned.
- *Eurodac has been the subject of both an audit conducted by the EDPS staff and a full fledged security audit carried out with the assistance of national experts provided by ENISA. So far, it demonstrated mostly the need for careful planning from one end to the other, as well as the need to have a cooperative relation with the audited body.*

2. Sanctions and other measures

Organisational aspects

- Is there a specific department in your authority responsible for sanctions and other measures? *No*
- If possible, provide staff numbers, professional experience and workload.
- Do you think that your resources (human and budgetary) and qualifications of staff fully satisfy your objectives?

Recent practice

- Please provide for recent figures for different types of sanctions and other measures available to your authority?

Not applicable

- Which sanctions or measures not yet available to you would be useful?
- Are decisions on sanctions or other measures systematically made public, and if so, how? If not systematically, on what grounds does your DPA make the decision to give the cases publicity?
- Please provide your own assessment on effectiveness of different sanctions and other measures, and publicity thereof.
- Which actions do you consider as especially noteworthy? Please describe results and lessons learned.

International cooperation for enforcement

The OECD report contains very useful information on that subject and concludes with a number of possible topics for further study. We would like you to consider the following questions, inspired to a large extent by the OECD report:

- Has your DPA been involved in 2005-2006 in cross-border enforcement activities? If so, what has been accomplished or learned?

Not applicable

- What would be in your view priority areas for cross-border enforcement cooperation?
- Does your authority in its current practice provide specific time and resources for cross-border enforcement cooperation?
- Do you think that practical tools should be developed (contact points, forms or procedures to request assistance from another authority, audit framework, common approach to reporting case results, others...) ?