



London initiative, follow up

Workshop on enforcement – 24 April 2007

REPORT

In the context of the follow up of the London initiative, the European Data Protection Supervisor (EDPS) hosted a Workshop devoted to enforcement issues in Brussels on 24 April 2007.

Participants

The DPAs attending were the following:

- Commission nationale de l'informatique et des libertés (France)
- Information Commissioner (UK)
- European Data Protection Supervisor (EU)
- Federal Privacy Commissioner of Canada (Canada)
- Garante per la protezione dei dati personali (Italy)
- College Bescherming Persoonsgegevens (Netherlands)
- Agencia Española de Protección de Datos (Spain)
- Datainspektionen (Sweden)
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Germany)
- Préposé fédéral à la protection des données et à la transparence / Eidgenössische Datenschutz und Öffentlichkeitsbeauftragte (Switzerland)
- Agencia de Protección de Datos de la Comunidad de Madrid (Madrid)
- Secretariat of the Joint Supervisory Bodies (EU).

The Privacy Commissioner (New Zealand), the Office for Personal Data Protection (Czech Republic) and the Generalny Inspektor Ochrony Danych Osobowych (Poland) were invited but unfortunately could not attend the meeting.

Purpose of the workshop

The London Initiative strongly emphasized practical and concrete approaches to making data protection more effective. The workshop on communication held in Paris had confirmed the value of this approach to launch discussions and to give a renewed impetus to the action of the data protection authorities.

The subject matter of this workshop on enforcement is in line with the spirit of the London Initiative, which aims at “*Communicating data protection and making it more effective*”. Indeed, effectiveness depends for a significant part on the enforcement activities carried out by the data protection authorities. The purpose of the workshop was to exchange information and learn about good practices in terms of enforcement at national and international level.

The workshop was intended to focus on three main issues:

Activities of DPAs in terms of inspections and audits: it is important to come to a good understanding of the DPAs' competences and activities in these matters. They may vary from fact-finding visits to fully fledged privacy and security audits; from case-bound and somewhat sporadic investigations, to the implementation of an exhaustive inspection policy. The emphasis for inspections may be on legal aspects or on technical ones. Some DPAs have a well established inspection or audit tradition, while others have recently launched activities in this area.

Further enforcement activities (interventions and sanctions): here also, experiences vary widely from one country to another. Some DPAs have wider powers to impose sanctions, but some others may obtain good levels of compliance through other means (such as publicity and pressure from the public). These approaches may have organisational consequences.

Cross border enforcement: In view of the volume of transborder data flows in many sectors, it is reasonable to assume that privacy risks are greater than ever in this field. The DPAs must evolve accordingly and think about ways to tackle this challenge. The OECD has recently published a study¹ on this topic, based partly on contributions by DPAs. The OECD was given an opportunity to present their findings during the workshop, as they are highly relevant for the work of the DPAs. The opportunity to create a network of enforcement officers was also discussed (see below).

Only a selection of cases has been extensively presented during the day, but there was an opportunity to share other experiences, questions, remarks and suggestions during the discussions.

Questionnaire and other documentation

In order to prepare the workshop, participating DPAs were asked to fill in a questionnaire sent in advance. The answers proved really interesting; they have been compiled and provided to all delegations at the workshop, and are attached to this report. They are obviously available to other interested supervisory authorities.

The questionnaire has, to a large extent, built upon the work already carried out by the WP29 task force on enforcement. This task force published in 2005 the national answers to a “Questionnaire on Requests for Information put to a controller, Complaints, Audits and Sanctions, and on their Implementation” (WP29 report). It contains exhaustive and relevant information on the legal framework for inspections and audits as well as on some practical aspects. The OECD report also contains useful factual information. Therefore, we have selected only additional questions focused on recent experiences and on the participants' views on different issues.

¹ Report available online at: www.oecd.org/sti/privacycooperation.

Launching of network of enforcement officers (experts) in DPAs

It has been decided to launch a network of staff in charge of enforcement in DPAs. The idea is not to duplicate work conducted in other groups (e.g. Enforcement task force of the WP29), but rather to provide for a list of resource persons in the DPAs. This network should be a tool for exchanging all relevant information not only on cross border enforcement activities, but also on domestic developments which could be of interest for everyone.

STRUCTURE OF THE REPORT

1. AGENDA	5
2. PRESENTATIONS ON ENFORCEMENT STRATEGIES AND EXPERIENCES	7
Introductory remarks - EDPS	7
2.1. LONG EXPERIENCES	7
a. Enforcing Data Protection : Learning Lessons - Dutch DPA	7
b. “Reflecting on a long established enforcement experience” - Spanish Data Protection Agency (AEPD)	9
c. Audit and Inspection Policy - Data Inspection Board (Datainspektionen), Sweden	10
2.2. MORE RECENT EXPERIENCES	11
a. Establishing a new enforcement policy: The Italian experience - Italian DPA (Garante)	11
b. From a notification-based to a multi-faceted model of supervision - French DPA (CNIL)	13
2.3. SPECIFIC EXPERIENCES	15
a. The Regulatory Action Division (RAD) within the Information Commissioner’s Office - UK DPA (ICO)	15
b. “The day after the audit”: Enforcement and further action - Madrid DPA (APDCM)	17
c. Experiences With Auditing International Organizations And Systems - Secretariat of the Joint Supervisory Authorities	18
d. Project on Cross-border Privacy Law Enforcement Co-operation: Update on work by the OECD	18
3. MAIN LESSONS LEARNT FROM ENFORCEMENT EXPERIENCES	21
4. ANNEXES:	
a. List of participants	
b. Presentations (in zip format)	
c. Compilation of answers to questionnaires on enforcement activities	

1. AGENDA

9:30am – 9:45am : Peter Hustinx' welcome speech and launching of the meeting

9:45am – 10:30am : Presentation by Ms Ite van Dijk, Head of the legal service of the Dutch DPA.

- Planning, organisation, performance and outcome of enforcement activities (audits, inspections, sanctions)
- Questions / answers

10:30am – 10:50am : Reflecting on a long established enforcement experience
Mercedes Ortuño, Joaquín Pérez, Spanish Authority

10:50am – 11:10am : Round Table

11:10am – 11:25am : Break

11:25am – 11:45am : Installing a new enforcement policy: the Italian experience
Francesco Modafferi, Italian Authority

11:45am – 12:00am : **From a notification-based to a multi-faceted model of supervision - How to deal with change?**
Yann Padova, Florence Fourets, Clarisse Girot, CNIL

12:00am – 12:10am : Round Table

12:10am – 12:30am : How to make the most of limited enforcement powers and ensure maximum impact of enforcement activities
Mick Gorrill, Information Commissioner's Office

12:30am – 12:45am : **Round Table**

12:45am – 2:15pm : Lunch

2:15pm – 2:30pm : Organising and carrying out inspections with an international team: lessons learnt
Peter Michael, Secretariat of the Joint Supervisory Authorities

2:30pm – 2:45pm : “The day after the audit: Enforcement and further action”
Emilio Aced Félez, Madrid Authority

2:45pm – 3:00pm : Round Table

3:00pm – 3:15pm : The OECD's activities in the field of cross-border enforcement of Data Protection

Michael Donohue, OECD

3:15pm – 3:45pm : **Round Table**

3:45pm – 4:15pm : Assessment of the meeting ; Follow-up work

2. PRESENTATIONS ON ENFORCEMENT STRATEGIES AND EXPERIENCES

Introductory remarks - EDPS

Peter Hustinx introduced the day, reminding that the raison d'être of the DPAs is to make compliance happen. There are different ways to achieve this: awareness raising is an important element; enforcement activities are another one (although they can dovetail since enforcement actions often call the attention of the public on data protection issues).

The EDPS also mentioned that this is an area where a lot of initiatives take place, and where several different groups are active: Enforcement Task Force of the WP29, OECD, Case Handling Workshop, Working Party on Police (development of a common audit framework). This workshop does not aim at duplicating work already carried out elsewhere but rather strives to be a source of inspiration for the stakeholders in this area. It will therefore focus mainly on practical aspects: lessons learnt from experience, available best practices, ways to deal with constraints of the legal framework, cultural changes brought in by the setting up of an enforcement policy...

Finally, a clarification was also needed on terminology, because of the various interpretations of terms used for this workshop. The workshop focused on enforcement as comprising mainly the inspection and sanction policy of DPAs (whether or not triggered by complaints). Inspection also has different meanings amongst the DPAs. For the purpose of the discussions, it was given a broad sense: an inspection/audit is, in essence, "the authority going to meet the reality".

2.1. LONG EXPERIENCES

a. Enforcing Data Protection : Learning Lessons - Dutch DPA

The morning session was launched by a presentation by Ite van Dijk, Head of the Legal Service of the Dutch Data Protection Authority

Ite van Dijk explained how the enforcement policy of the College was launched and what its evolution was over the last years. She insisted that she would not paint too positive a picture of it, since there is much to gain also by sharing difficulties and challenges, not only successes. She pointed in all cases to the lesson that was learnt at this occasion.

How it started: it is underlined that the starting of the enforcement policy (in 2002) is based on a clear and firm decision of the commissioners. It has an impact on the organisation in terms of human resources: it led to the hiring of new staff, but in order to have this new activity well accepted by all staff, it is suggested that having a mix of "old" and new staff dealing with enforcement is advisable.

- Lesson: embedding of enforcement activities within the authority needs a firm commitment from the management. The launching of this policy must be accompanied by adequate staffing.

Selection of investigation objects: The selection of investigation objects was made at first on the basis of the notifications, or rather, the obligation to notify. After analysing the situation, a last warning to underrepresented sectors and governmental organisations was sent. Finally, a random selection of 50 data controllers operating in 4 sectors was made.

- Lesson: when compliance is low and you take samples, a neutral statistical method is required. Be prepared to justify your method of selection because everyone is going to contest it. Keep a good record of your considerations for any court cases (which you should expect).

Communication as multiplier: Publicity (press releases, newsletters and interviews) was used as incentive to increase compliance. Naming and shaming could in some cases work as a multiplier too. Publicity was also used as means to transparency and to account for the investigation policy (regular reports on the website).

- Lesson: small investigation samples can have a great impact (the number of notifications increased from 5.000 to 20.000 within 2 years); a well-chosen investigation promotes the issue of data protection and in addition brings the DPA political and public support.

Establishment of enforcement activities is a long term project: Rough times can be encountered and persistency is key. Lawsuits, administrative rulings might go contrary to the policy. Special attention must also be brought to keeping experienced, skilled and motivated people in the organisation.

- Lesson: Beyond careful planning, an enforcement policy also requires permanent attention.

New method: repeated investigation: The Dutch DPA selected specific sectors for investigation, sent first questionnaires, and then carried out in a few cases spot inspections. The outcome revealed extremely low compliance with the obligation to inform. A first follow up action consisted in a letter of explanation to all agencies with sharp warning. It was followed by a second action: inspections on the spot and if necessary penalties.

This method was applied in different sectors.

- Lesson: data protection norms are not always clear to the data controllers; investigations in two rounds can be used to elaborate the norms in each sector or activity.

Plans for 2007/2008

The new projects for these two years include in particular:

- Use of a new investigation method: electronic questionnaires
- Elaboration of norms by soft law/guidelines (e.g. internet)
- Political lobby for publication as penalty in the Data Protection Act
- Further development of a system for compliance and risk analysis
- Combined investigation with Health inspection
- Strong interaction between enforcement and communication (enforcement targets to enhance the social basis for data protection)

- Lesson: Enforcement in the Netherlands is still under development; experimenting with several methods seems to be fruitful.

b. “Reflecting on a long established enforcement experience” - Spanish Data Protection Agency (AEPD)

Competences: The AEPD has supervisory responsibility over all issues related to protection of personal data in the private sector as well as in the public sector, with the exception of the local public sector of Madrid, Cataluña and País Vasco. The AEPD “acts with full independence of the Public Administration in the exercise of its functions” but, as a part of the administration, has to comply with procedural and formal rules governing the administration. That means, i.a. that the AEPD has to handle every complaint it receives, which represents a heavy workload. The AEPD would like to have some flexibility in this regard; this concern is shared by many other DPAs (see below).

Preventive action (i.e. guidance on compliance by industrial sectors, ad hoc consultation, awareness raising, ex officio audits of private and public sectors) constitutes around 20% of the enforcement activity of the AEPD, while reactive action (complaints handling, leading or not to an inspection) would constitute around 80 % of the enforcement activity.

Reactive enforcement (based on complaints): The AEPD has the investigative and enforcement powers of the State; as it can impose sanctions, it must ensure due process to all parties. It has a number of tools to handle complaints (i.a. inspection in situ, fines, possibility to block the processing).

Complaints are dealt with by an Inspection Unit and an Instruction Unit, working closely together, but with clearly defined roles. The inspectors check the facts, but do not make legal evaluations (except in issues related to security legislation), while the instructors make legal evaluations. The inspectors and instructors carry out regular cross training.

Preventive enforcement: Ex officio audits are conducted by the AEPD according to a well defined procedure, from the choice of a sector and the selection of a representative sample of the sector to the elaboration and publication of mandatory recommendations (see presentation in annex). In each case, an audit plan is created, which allows for a relatively standardized procedure. Contact is taken with a high level person in the audited organisation.

Sanctions: Both “hard” and “soft” sanctions (injunctions, publication of decisions, communication to ombudsman...) are used, in practice, to ensure compliance in a particular case and promote a culture of compliance.

Fines cannot be imposed on the public sector, because the taxpayer would end up paying twice (same situation in several other countries).

The following elements are considered a key for effective enforcement:

1. Competence and Powers: Effective powers of investigation by law (check-up in situ ; direct access to computers; ability to compel data controllers to collaborate in investigations.)
2. Human Resources: Skilled technical (IT) and legal experts, working together in permanent cooperation.
3. Organizational Factors:

- Definition of roles and responsibilities among inspectors (technical experts) and (legal) instructors.
 - Team effort (several inspectors working together in a case..)
 - Cross training inspectors-instructors (technical/legal expertise)
4. Expertise: Since 1997 developing audits in all sectors
 5. In performing the audits:
 - Selection of representative sample.
 - Having high level contact person in the organization as interlocutor
 - Direct check-up in the audited organization
 6. Competence to request and provide International Enforcement Cooperation, since a great number of cases concern the Internet.

c. Audit and Inspection Policy - Data Inspection Board (Datainspektionen), Sweden²

Ex officio audits: An audit may be initiated on the Data Inspection Board's own initiative, after complaints from individuals or a tip from mass-media, public authorities, organisations and others. An audit shall above all be directed towards processing operations that are considered sensitive from a privacy point of view:

- processing involving a great deal of data concerning one person,
- processing concerning many people
- new phenomena where there might be a risk of infringement of privacy.

Other relevant criteria include:

- processing of sensitive personal data, for instance, data concerning legal offences or crimes and opinions about a person
- the dissemination of data,
- the risk of damage or misuse, if the processing is indiscreet
- if the data subject is in a position of dependence in relation to the data controller.

As to the processing of personal data carried out by public authorities, big companies or big associations, audits may be considered even if it is not a matter of processing like the kind mentioned above. These data controllers are expected to comply with the Data Inspection Board's decisions and disseminate its point of view to other public authorities, companies or organisations. An audit shall normally not be initiated when the processing of personal data already is subject to a police report or to a court trial.

Audit or inspection after a complaint: An audit or inspection shall be considered in the following cases (after an assessment of the merits of the complaint):

- In case of serious deficiencies
- If the data subject has tried but not been able to bring about a rectification on his own
- If the processing has been carried out by public authorities, big companies or big associations
- When the individual person is in a position of dependence in relation to the data controller

If there is a personal data protection officer (DPO), a copy of the audit letter or the inspection notice shall be sent to the DPO for information.

² Written contribution

If the deficiency is less serious the Data Inspection Board shall consider directing the data subject to require a rectification himself. The complainant will then be informed about what rules apply and urged to request for a rectification himself. The data subject will also be directed to the DPO if any.

The Data Inspection Board shall strive for a uniform assessment of the merits of complaints. The persons responsible for a certain sector should give a preliminary assessment on the specific case of whether or not an audit shall be initiated. In doubtful cases the official in charge shall consult his audit manager/equivalent.

Audit after a tip from mass-media: An audit shall be initiated, after consultation with the audit manager/equivalent, in cases of evident infringements on data protection legislation or if it is feared that there will be such infringements. Alternative measures may be considered for instance when the data controller has made a rectification such as an announcement on the website.

Policy for audits and inspections in different sectors: Separate policies shall be drawn up, if necessary, for sectors with many complaints.

Choice of audit method: Audits can be carried out as field inspections, audits through questionnaires or written procedures. The Data Inspection Board shall choose the most efficient method to investigate the case in question.

A field inspection shall be approved of by the audit manager/equivalent and be chosen when the issue at stake is best investigated by a visit on the premises of the audited controller, for instance when the Datainspektionen has many questions and needs to see how it functions practically or when the IT security is especially important.

An unannounced field inspection shall only be chosen in exceptional cases and be approved of by the audit manager. This can be appropriate when there is a risk that the data controller does not give correct information or continues the unlawful processing.

An audit through a questionnaire shall be chosen when the Data Inspection Board wants to know what the protection of privacy is like in a certain sector or how common a certain kind of processing is. A questionnaire can also be used as basis to select suitable controllers for field inspections.

Written procedure shall be chosen when the case can easily be investigated by way of correspondence.

2.2. MORE RECENT EXPERIENCES

a. Establishing a new enforcement policy: The Italian experience - Italian DPA (Garante)

Evolution of the inspection's activity

The Garante was concerned with the presence of three inter-related phenomena (as already noted by the European Commission):

- An under-resourced enforcement effort and supervisory authorities with a wide range of tasks, among which enforcement actions have a rather low priority

- Very patchy compliance by data controllers, no doubt reluctant to undertake changes in their existing practices to comply with what may seem complex and burdensome rules, when the risks of getting caught seem low
- An apparently low level of knowledge of their rights among data subjects, which may be at the root of the previous phenomenon

It decided to tackle these phenomena by increasing noticeably the enforcement activities; in particular, since 2005 Garante has increased the ex officio inspection activity, which has required a much more proactive attitude than in the past.

These activities are performed by a specific Department which can investigate criminal offences concerning data protection and related matters, availing itself of staff acting in the capacity as judicial police officers, collaborates with judicial authorities (both criminal and civil) and may, finally, request co-operation of police forces (in particular, a Memorandum of Understanding was signed with the Guardia di Finanza).

Inspection program

In order to address the office in this activity the Garante fixes, every six months, the guide lines of the ex officio activity.

The program determines:

- the total number of ex officio inspections that have to be performed in the six-month period
- the different kinds of inspections and the number for each category
- the specific object of the inspections that have to be performed by the Department

How to increase inspection activities?

The Garante avails itself of the assistance of the Guardia di Finanza (which collaborates with the Authorities in charge of supervising sensitive and strategic sectors of the economy, such as the free market, communications or data protection). This cooperation, established by numerous memoranda of understanding (MoU), is ensured also by means of dedicated Special Units dealing with these sectors.

The MoU sets out cooperation between the Guardia di Finanza and the Garante as regards:

- Gathering data and information on the entities to be controlled
- Assistance in relationships with judicial authorities
- Participation of own staff in accessing databases, in inspections and audits, and in all other controls as performed at the premises where the processing takes place
- Discharge of the tasks committed in order to establish commission of criminal or administrative offences

A new special unit of GdF is in charge of data protection inspection activities. It is composed of 40 officials and located in Rome (but active throughout the country). The inspectors are specialised in data protection and are recruited on the basis of different skills: audit, relationship, legal and technical. They receive a special training when they start in their job as well as continued training over their career. On top of this special unit, regional units may also be involved in inspections in less sensitive or complex cases.

The Inspection policy of the Garante sets out criteria to allocate inspection work, based on the complexity and sensitivity of the matter. The cases considered highly sensitive or complex are dealt with by the Inspection Department in the Garante's Office; the cases with medium

sensitivity are allocated to the special unit of the Guardia di Finanza, and finally, the cases with low sensitivity are dealt with by the local units of the GdF.

b. From a notification-based to a multi-faceted model of supervision - French DPA (CNIL)

Evolution of supervisory activities: From 6 January 1978 to 6 August 2004, CNIL's model of supervision mostly relied on prior notification (private sector) and prior checking (public sector). Enforcement powers were scarcely used; internal organisation and staff culture reflected this policy.

Since August 6, 2004 (new DPA), CNIL's inspection powers have been reinforced: possibility to have access to all professional premises, to request all necessary documents and to take a copy, to have access to all IT systems and to request transcription of the data, with some restrictions (medical files state security files). The number of inspections has increased almost tenfold from 2001 to 2006, with some very prominent cases (e.g. e-ticketing scheme in the Paris metro; electronic health records; banks, etc.).

Assessment of CNIL's inspection policy

- Inspections now have a major role in CNIL's global policy
- An important factor of credibility (although more staff would be needed to meet expectations)
- One small inspection can have big consequences (e.g. inspection at one hotel => the group has launched a worldwide audit on its data protection practices)
- Direct link to sanction powers and policy

Sanctions : what can CNIL do? (with *figures since 2005*)

- Warning ("avertissement"): *14 cases*
- Compliance order ("mise en demeure"): *126 cases*
 - If non compliance with such an order:
 - Financial sanctions (except State): up to €150.000; if repeat offence: €300.000 or 5 % of turnover (max €300.000): *15 cases, for €228.300 in total*
 - Issuance of order to stop processing: *9 cases*
- In case of emergency:
 - interruption of processing (3 months max.)
 - blocking of data (3 months max.)
 - Information of Prime minister if public security file involved
 - If particularly serious offence, President can ask the judge to order any necessary security measure
 - Withdrawal of authorisation
 - Possibility to refer cases to the Public Prosecutor (not a sanction as such) : sanctions up to 5 years imprisonment and €300.000

Sanctions may be appealed to the Council of State.

Sanctions: how does it work?

A specific committee within the CNIL has been created by the law: the « restricted committee » (« formation restreinte »), composed of President, 2 VPs, 3 members elected by Commissioners among themselves. This committee is the only competent organisation within CNIL to impose warnings and financial sanctions (not other sanctions).

In case of emergency, the same sanctions may be imposed by President + VPs (« bureau »)
Since Sept. 2004: a « Sanction Unit » is created on CNIL's staff to feed the agenda of the restricted committee.

Many formal rules of procedure need to be followed to ensure due process

Assessment of the use of sanctions

-Globally very positive results:

- Compensates the lack of enforcement of DP issues in the courts for want of time, resources, DP awareness (e.g. on spam), but also because of issues of costs, length of judicial procedures, etc)
- Helps being taken seriously by data controllers
- Great medium for communications and awareness raising
- Has raised the level of responsibility within data controllers' organisations where data protection issues are dealt with

However:

- Imposing sanctions is not an easy decision to take:
 - Heavy consequences for controllers
 - Need to ensure consistency between cases, and proportionality: there are risks for the image of DPA as well!

Impact on methodology and procedures

- A real enforcement policy dramatically changes the way CNIL used to work (greater formalism, a huge number of major policy questions have to be answered in a very short period of time, major change required in the staff culture, etc.)
- It has an impact on all the other aspects of CNIL's work (e.g. notification, communication, complaints, etc.: need to develop a horizontal way of thinking in the organisation)

Impact on internal organisation

- Creation of a dedicated inspection department (2001) and of sanction unit (2004)
- Specific requirements in terms of staffing (e.g. for inspections: former policeman; mix of lawyers and IT experts)
- Necessary to ensure good coordination with other departments (legal; complaints) to detect cases for inspections & sanctions and to set up a yearly policy – requires building horizontal thinking
- A reorganisation is pending to ensure the proper implementation of these policies

Some interrogations in terms of strategy

- What sectors of activity should be concerned by inspections and sanctions?
- Should a distinction be made between failure to comply with essential or formal requirements (e.g. breach of access right vs. no notification)?
- When is a warning an adequate sanction; when should we rather use compliance orders?
- How to ensure consistency between decisions to apply sanctions ourselves and decisions to refer cases to court?
- Which relations with the Public Prosecutor's Office?
- What are the relevant criteria to set the level of a fine?

Some shortcomings in the law

- Main sanctions powers (ie injunction to put an end to the processing and financial sanctions) must always be preceded by a compliance order, which may hinder the effectiveness of CNIL's powers
- Maximum amount of 300.000€ should be increased (not sufficient for big data controllers)
- No financial sanctions against controllers in the public sector : questionable under circumstances
- Difficult in practice to publish decisions yet « naming and shaming » is very efficient.
-

2.3. SPECIFIC EXPERIENCES

a. The Regulatory Action Division (RAD) within the Information Commissioner's Office - UK DPA (ICO)

Organisation: The RAD is comprised of four units:

- Remedies,
- Investigations,
- Enforcement
- Audit

The majority of cases forwarded to RAD pass through Remedies where a judgement is made on the type of regulatory action which may be needed. The majority of cases referred are dealt with by Remedies staff.

Some figures: During the period 1st April 2006 to 31st March 2007 1300 cases were referred to Remedies:

- Remedial action was taken in approximately 300 cases (25%),
- In a further 25% no action was required
- 650 (50%) were referred for investigatory or enforcement action

Examples of RAD action

Remedies: Data Subject Access Request to Liverpool City Council: A former employee of Liverpool City Council (LCC) made a subject access request to the council asking to be supplied with personal information about her which was held by the council. Following her request LCC provided some information but the data subject complained to the ICO that she had not been supplied with all the information which was held by the council.

The ICO commenced an investigation. LCC failed to respond to written requests for information. As a result the ICO issued an information notice requiring the council to provide them with specified information (failure to comply with an information notice is a criminal offence contrary to Section 47 of the Act). No response was received and a prosecution was brought against the council.

LCC appeared at Liverpool City Magistrates Court in December 2006 where a plea of guilty was entered. In sentencing the Council the District Judge at Liverpool Magistrates' stated that the Council had shown an "appalling breakdown of communication" and "a clear lack of compliance with the Data Protection Act 1998". The Council were fined £300. The council agreed to allow the ICO to audit their data protection processes.

Investigations: In November 2006 a married couple pleaded guilty to 25 offences of unlawfully obtaining personal data following an ICO investigation. They had obtained personal information from a number of organisations by 'blagging' the information. They had

purported to be employees of various organisations which enabled them to unlawfully obtain the personal information.

They were fined a total of £7,500 and ordered to pay £3,694 costs.

The investigations have shown that there is a widespread demand for personal information. At the present time the investigations unit are investigating 23 different complaints relating to the unlawful obtaining of personal data. These current investigations involve many hundreds of offences.

Proactive Investigations

In August 2006 the ICO were contacted by a freelance journalist. Since February 2006 he had made visits to several Banks and a Post Office in and around the Southampton area and recovered various items of personal information from waste bins placed at the rear of each premises. In all cases the bins were insecure with open access to the public. After a lengthy ICO investigation 11 Banks, the Post Office and the Immigration Advisory Service were required to sign formal undertakings to comply with the Data Protection Act and warned that failure so to do could lead to future prosecution.

All the organisations subject to the undertakings agreed to allow the ICO to conduct a themed audit of their policies and procedures relative to the disposal of personal information.

Enforcement

Prior to 2002, individuals had no choice over whether their personal details from the electoral register were sold on to other organisations. After that date individuals could opt out of the public register. Complaints were received from individuals who had subsequently opted out of the public register but whose details were freely available on the website.

B4usearch.com allowed individuals to search the pre 2002 electoral registers and obtain name and address details of some individuals who had subsequently opted out of the register.

The ICO considered that this was unfair processing. In July 2006, the ICO issued an Enforcement Notice against the website B4usearch.com ordering the directors of the company to stop using personal information from electoral registers published before 2002.

Audit

During the period 2006/2007 effectively 8 audits were conducted. The audits were conducted at three NHS Trust organisations, two local authorities, a police force a higher education college and a government department.

The team has also undertaken a survey of Medical Health Insurance Companies as a joint piece of work under the auspices of the Article 29 Working Party.

Audit are also preparing to complete themed audits of the organisations investigated for their following the finding of personal information in waste bins.

Audit is an area which is seen as an increasingly important function of the ICO. The ICO is currently seeking to expand the audit unit in anticipation of an increase in the numbers of future audits.

Powers

The ICO consider on occasions that their powers to change the behaviour of some data controllers are not sufficient. Ideally a means to fast track some data controllers to court to stop/prevent such behaviour quickly and impose a realistic punishment is considered necessary.

More importantly even, ICO is not allowed to go on inspection without being invited by the audited party. The ICO considers this a major limitation to their enforcement powers and seeks to obtain a legislative action to amend the DP Act in this regard.

NB: The ICO also has the power to issue a special report to the Parliament and used this power once so far (the “What Price Privacy” Report, which has a huge impact).

b. “The day after the audit”: Enforcement and further action - Madrid DPA (APDCM)

Enforcement activities: The APDCM has at first focused on awareness raising activities, which constituted roughly 80% of its activities, as compared to the enforcement activities (20%). This focus is shifting now towards more enforcement activities. The APDCM conducts two types of enforcement actions:

Reactive:

- Complaint driven. It covers both the investigation of possible breaches to the data protection legislation and a special procedure provided by the Spanish legislation when the denial of the rights is involved. In the first case these reactive actions take the form of an investigation, which can lead either to the closing of the case if no breach is detected or the starting of infringement proceedings, with eventual sanction to the controller. In the second one, the usual end is a decision of the DPA establishing whether the data subject has the right to access, object, amend or cancel his or her data. If the data controller complies with the decision, no further infraction proceeding is conducted
- Ex-officio investigations of specific possible breaches.

Proactive

The aim here is not to seek sanction for breaches, but to gain a better knowledge of reality and to improve existing situation by different means (advising data controllers...)

There are Ex-officio Sector Actions (Scope limited to certain aspects of the data protection principles or specific types of personal data. e.g. processing of genetic data in public hospitals) and ex-officio Sector Inspection Plans where a systematic compliance review is conducted (e.g. Social services).

For the inspection of Social Services, a model plan has been followed, comprising all steps from study to press release and diffusion through datospersonales.org. This plan has been officially adopted by the Steering Committee of the APDCM, which emphasise again the need for a clear commitment of the management.

Follow up actions of the inspection

Drafting of Conclusions and Adequacy Instructions

- Adoption by DPA Director
- Individual ones sent to audited controllers
- General ones: Publication in the Regional Official Journal without identification of concrete controllers

Press release and diffusion through datospersonales.org

Forwarding of results to

- Regional Parliament
- Data Protection Advisory Council

Special mention in Annual Report (Stress on the inspection during presentation to the MPs and to the media)

Specialised awareness raising actions/targeted training sessions for small groups (Stress on inspections results as an improvement tool).

- One day seminar focused on Social Services (Presentation of results, analysis of deficiencies, recommendations for improvement,...)
- Specialised leaflets addressed to target groups in this sector (Elderly people, users of Social Services,...)
- Updating of FAQs in website

This presentation highlights the fact that inspections are not an end in themselves, but serve the broader purpose of enforcement and awareness-raising. Inspections can lead to a better understanding of the sector for the DPA and a better understanding of data protection obligations for the sector.

c. Experiences With Auditing International Organizations And Systems - Secretariat of the Joint Supervisory Authorities

Competences: The JSAs are in charge of joint supervision including joint audits of the following systems: Europol, Eurojust, Schengen Information System and Customs Information System. They have conducted several audits in these organisations, in particular in the premises of Europol and the Central Unit Schengen (C-SIS).

Definition of the scope and object of the audit is of course crucial; it is helped in these cases by the legal framework who gives indications as to the investigative missions and competences of these authorities.

Choosing the method for inspection is sometimes challenging: inspections are led according to international standards, but IT auditors have different backgrounds and experience, and use different specific methods. However, it is a very positive experience to bring together all this expertise. In these inspections, a specific period of time is always allocated to define the inspection method and to allow the auditors to know each other. The positive outcome of all this is that auditors also learn from one another.

Another positive result is that a good, trusting relationship has been built with the audited institutions, especially with Europol. Europol now wants to be audited, because they see this as a chance to get specialised advice on data protection issues, free of charge! Moreover, the actions requested by the JSAs in their inspection reports aim more at improving the situation than at sanctioning.

Regular inspections are good for maintaining awareness: when they know they are likely to be audited frequently, data controllers will probably keep data protection higher in their agendas.

d. Project on Cross-border Privacy Law Enforcement Co-operation: Update on work by the OECD

Overview of the project

The Working Party on Information Security and Privacy, through an expert sub-group chaired by Jennifer Stoddart, and including DPA representatives, EC and Council of Europe, is in charge of the project. First, a fact-finding phase ended in a "Report on Privacy Enforcement"

(October 2006), based on Questionnaire responses from 22 countries, describing existing enforcement authorities and systems, and identifying cross-border challenges needing further work.

The ongoing second phase is the development of a policy response, consisting in a Draft OECD Council Recommendation, presented during the workshop, with some tools. This phase should be completed by June 2007.

Findings: How are privacy laws enforced?

Privacy enforcement authorities are commonplace (today: nearly all OECD countries have DPAs), but structures as well as enforcement powers and processes vary widely. Information gathering powers (onsite inspections, production of documents, audits) as well as sanctions, remedies or outcomes (declare violations, publicity, enforceable orders, fines, compensation for individuals) are different from country to country. The question is: to what degree do these variations impact enforcement co-operation?

Existing cross-border challenges: they concern mainly

- mutual assistance (information sharing, investigative assistance,...),
- enforcement powers (availability of sanctions and remedies providing adequate deterrence),
- identification of common enforcement priorities
- need for continued information gathering (cross-border complaint and case trends).

The OECD initiative

-This initiative builds on existing activities and initiatives

- Enforcement activities (few cross-border cases, an increasing number of cross-border audits/inspections)
- International instruments (with an enforcement component): CoE Convention 108, EU Directive 95/46/EC, APEC Privacy Framework, EU-US Safe Harbor, AUS-NZL, ESP-USA
- Less formal networks (without an enforcement focus): International Commissioner's Conference, IWGDPT, APPA, Iberoamerican
- Examples from other areas with successful enforcement mechanisms : spam, consumer protection, competition

-The draft Policy Framework

An OECD Council Recommendation is non-binding, but represents a serious commitment to implement (especially since it is approved at ambassadors level). It blends high-level policy objectives with key elements for good co-operation, leaving the implementation details to Member States and their authorities. Non-OECD countries are invited to collaborate with OECD members in this framework.

The key actors in this initiative would be the DPAs (who in principle are endowed with the power to investigate or pursue enforcement proceedings), but also the Criminal law enforcement bodies, Privacy officers in organisations or Private sector oversight groups would have an important role to play.

The focus of draft Recommendation is on violations most serious in nature. Moreover, it is primarily aimed at private sector (but can include public sector) and is not intended to interfere with government activities related to sovereignty, security or public policy. It would recognise that authorities may decline or limit assistance, where the request is outside the scope or otherwise inconsistent with national laws, important interests or priorities

What is needed for cross-border cooperation in Privacy Enforcement:

Domestic Measures: you need to have

- the right domestic arrangements to co-operate internationally (which would imply in some cases a review of laws, procedures)
- effective powers and authority: sanctions and deterrence, investigative powers, the right to implement corrective action.
Ability to co-operate: to share information and to provide assistance (e.g., obtain documents or statements)

How does it work:

The OECD Initiative identifies the key elements for successful Mutual Assistance

- Requests for assistance
- Preserve the confidentiality of non-public information
- Respect the purpose specified when information exchanged
- Co-ordinate investigations to avoid interference
- Referral of complaints, notifications

Would call for collective initiatives in support of mutual assistance

- Contact points, information about laws
- Sharing information about outcomes
- Foster the establishment of an informal network of authorities

And co-operation with other stakeholders

- Criminal authorities, privacy officers, civil society, business

In addition to the draft Recommendation, the OECD has been working to develop Practical Tools:

Contact List of officials in charge of enforcement activities

- Single national point of contact via a designation form
- Internal list (with complete contact information)
- Public list (can exclude personal contact information)
- Co-ordinate with contact lists in APEC, elsewhere?

Request for Assistance Form

- Identifies key categories of information to be provided
- Ensure careful preparation: helps ensure that preliminary investigation has been conducted
- Flexible: can be adopted to fit the situation (referral, audit, etc.)
- Not Duplicative: doesn't ask for what is readily available elsewhere

It is also considering developing a Restricted-Access Web site

- Access restricted to privacy enforcement authorities
- To permit discussion on actual cases, general issues
- Could be supplemented by a public section

3. MAIN LESSONS LEARNT FROM ENFORCEMENT EXPERIENCES

a. Preliminary remarks

A clear conclusion of the workshop is that most DPAs are going through a phase of huge change; their focus has long been on the building of a much needed legislative and regulatory framework. But when this framework is complete, there is a need to make it effective, by communicating better and taking enforcement action when needed.

Some DPAs have started a while ago to develop their enforcement policy, while some have a shorter experience, or are still building it. The workshop allowed the sharing of experiences of DPAs in different stages of development of enforcement policy, which proved enlightening. It is also evident that, though national contexts and issues may differ, the DPAs were struggling with common issues, and have also a common assessment of success factors and challenges.

b. Key elements of an enforcement policy

1. The launching of an enforcement policy requires a strong and continued commitment by the management. Implementing enforcement action implies changes in working methods and habits of the organisation as a whole, and cannot be done without support from the highest level. A clear policy must exist inside the organisation.

2. Enforcement requires an involvement (of various degrees) of all the staff, also those who are not in charge of inspections/sanctions. For instance, different units within the organisation must be aware of the cases that should be the object of enforcement action and warn the inspection unit; cross-training could be organised between legal and IT officers

3. Having some staff highly skilled in auditing and on other related aspects of enforcement (staff with contentious procedure background for sanction procedures) and keeping them seems to be at the same time a prerequisite and a challenge. Another interesting option is to make use of that expertise from another public body (like the Garante and the Guardia di Finanza).

4. A strategic planning of enforcement activities is an absolute necessity. DPAs have different ways to plan inspections and audits, and communicate about it in different ways. It has been considered useful to mutually inform each other of strategic planning so as to learn from each other and to identify cross border priorities. This exchange of work programmes could concern not only the planned inspections but also other strategic activities of DPAs, whether in terms of communication, notification policy, promotion of good practices or codes of conduct, etc.

5. An effective enforcement policy should reflect the increasing needs for authorities to be able to work together on cross-border cases. This is sometimes experienced as difficult, because of information sharing limitations and other legal and practical obstacles. At the same time, cross-border cases can provide for a welcome opportunity to share expertise and best practices, which should be encouraged.

c. Challenges

1. One of the most important challenges for the DPAs comes from constraints stemming from their respective legislation. In particular, many DPAs struggle with the legal obligation to deal

with all incoming complaints, regardless of their merits or the seriousness of the breach they denounce. With no opportunity to prioritize, and limited resources, many DPAs find themselves incapable of dealing with real priorities. They do much more reactive enforcement than proactive. It should be noted, however, that the legislation could be interpreted in a more relaxed way. Directive 95/46/EC for instance provides that DPAs must “hear” all complaints, which doesn’t mean that they have to be dealt with in the same way, let alone extensively, if they are not relevant.

Moreover, DPAs who are allowed to prioritize find it difficult, for various reasons:

- a criterion for priority such as the “seriousness of the impact” can be difficult to assess;
- sometimes, the possible effect of an enforcement action in terms of communication strategy would outrank a more factual criterion such as the number of data subjects concerned: the choice of a target for enforcement action is also a politic exercise;
- very often, staff is reluctant to reject a complaint: they want to be helpful on the one hand, and on the other hand, they do not dare taking this responsibility.

The participants agreed to pursue the reflection on this aspect and to exchange further views on this question.

2. Questions arose with regard to the “naming and shaming”. The publication of the names of inspected or sanctioned organisations is not always legally allowed. A majority of participants found that naming and shaming had a great impact, not only on the organisation in question, but very often, on the whole sector. Others found it an inefficient method, since the impact, in the private sector, at least, is minimal (the impact on the market is non existent and companies sometimes don’t care). Experiences in this regard could be shared further.

3. More generally speaking, it was pointed out that it is advisable to maximise the impact of audits/sanctions by various means: publication of results, engaging in synergies with other stakeholders (consumer associations, patients associations, etc). The question of the real impact of fines and the desirability of increasing fines has also been discussed.

d. Positive aspects of enforcement

Enforcement activities have a number of positive consequences:

1. They raise awareness on data protection issues. Even if no audit is actually conducted, the awareness of data controllers that they could be audited at any moment encourages them to maintain their processing operations in compliance with the applicable legislation.

2. The DPAs can appear as advisors, experts who help data controllers doing the right thing. This may encourage them to call on the DPA as an advisor. More generally, enforcement helps being taken seriously by data controllers.

3. It raises the level of responsibility within data controllers’ organisations where data protection issues are dealt with: in many cases, they are now dealt with as a “compliance” issue at policy level, rather than as a legal issue only.

4. Sometimes, in the course of an audit, auditors may discover that the audited body actually has very good practices, or found a creative/technical/legal solution for a problem which affects others as well. Good practices can be identified and promoted widely at this occasion.

5. After an audit, the need for information on specific subjects or targeted to specific groups can also be identified. Information campaigns can therefore be much more targeted and cost-effective. Enforcement is a great medium for communications and awareness raising.

6. Enforcement actions help compensate the lack of enforcement of data protection issues in the courts because of issues of costs, length of judicial procedures, etc., but also sometimes for want of data protection awareness (e.g. on spam).