Recent examples of enforcement actions carried out by data protection authorities

(January 2005)

Belgium

Further to numerous complaints from debtors, and in agreement with the national bank, the Belgian DPA has been given direct access to the database to check before and after dealing with the given bank.

Proactive enforcement strategies

The Belgian DPA has been working closely with representatives of the Belgian Direct Marketing Association, in order to improve provisions of their code of conduct concerning data protection.

One field considered relevant for undertaking enforcement action would be the sector of banks and insurances where the DPA has identified problems related to the transfer and reuse of data for incompatible purposes. List broking and in particular collection of data by list brokers would be another issue to deal with on a wide scale.

Czech Republic

Sanctions were imposed in the following sectors:

- Banking sector: collection of personal data from potential clients and processing of them without data subject's consent;

- Municipal administration: publication of personal data of persons who were subject of negotiations during municipal authorities meetings by way of making their resolutions public (€ 1.290);

- Educational system: failure to meet inevitable measures against unauthorised and accidental access to personal data of students;

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 15 of Directive 2002/58/EC. The Secretariat is provided by:

Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: http://europa.eu.int/comm/internal_market/privacy/index_en.htm

- Recruitment of personnel: processing of personal data of job seekers incl. sensitive data without their explicit consent and in a manner hurting human dignity; lacking measures against unauthorised processing of personal data (€ 16.129);

- Telecommunications: formal insufficiencies of the consent of customers and further persons addressed in relation with an offer for services and business;

- Financial sector: processing of personal data of customers and credit applicants; storage in a database even after the justifiable purposes for processing ceased to exist; formal insufficiencies of the consent;

- Travel industry: disclosure of personal data by sending away travel agreements containing personal data of all travellers (€ 194).

Proactive enforcement strategies

Sectors considered relevant for undertaking enforcement action are banks, insurance and other financial institutions; direct marketing companies and advertising agencies; telecommunication operators; city and municipal authorities, social-care and health-care administration; personnel recruitment agencies; distribution companies; and entities responsible for unsolicited commercial communications.

Denmark

In a case where a public psychiatric hospital had sent an unencrypted e-mail containing sensitive data regarding a data subject's health and criminal record to an employed psychiatrist, and which were forwarded due to a computer virus to a large number of third-parties, the DPA requested to be informed of which measures the governing public authority were taking to remedy the situation and to prevent similar situations from occurring in the future.

In a case where a private webpage was publishing so-called spy-photos, containing images of persons partially or fully naked who did not know they were being photographed, the DPA instructed the owner of the webpage, to cease from processing the pictures on the internet immediately, and forwarded the matter to the relevant police authority for criminal investigation.

In a case concerning access to credit information in order to slur an opponent in connection with a political campaign, the DPA stated upon request that the processing of such data must only take place for valid purposes; use in an electoral campaign is not considered such a valid purpose. The case went before the courts, and it was held that the accessing was in contravention of the Danish Data Protection Act, and the person concerned was fined 5.000 dkk.

Proactive enforcement strategies

As illustrated by the above mentioned cases, it is the strategy of the Danish DPA to remain aware of cases being mentioned in the media which may give rise to data protection issues. When such cases are identified, the DPA will on many occasions intervene on its own initiative.

The DPA is currently placing particular enforcement focus on headhunting firms operating in Denmark without the required permission from the DPA (cf. section 50, subsection 1, no. 4 of the Danish Data Protection Act).

Finland

The Data Protection Ombudsman applied to the Data Protection Board to prohibit the processing of personal data by a company that collected taxation information on individuals and published them regionally as a "magazine" and by another company, owned by the same circles, which offered taxation information based on information on the said publication as an SMS service. The Data Protection Board returned an unfavourable decision, mainly on the basis of freedom of speech. The Data Protection Ombudsman has appealed the decision to the administrative court. The appeal included a request that the competent administrative court request a preliminary ruling from the Court of Justice of the European Communities.

Proactive enforcement strategies

Because many website providers neglect their duty to provide data subjects with information on the processing of personal data collected in e-transactions and services, the Office of the Data Protection Ombudsman has been distributed brochures to data subjects and data protection guides to municipalities, central administration, non-governmental and labour organisations and trade and employer's associations, among others.

During 2004 two new Acts have been entered into force in the field of data protection. One of them is the Act on Data Protection in Electronic Communications that will safeguard confidentiality and protection of privacy in electronic communications. The other Act is dealing with the Protection of Privacy in Working Life. The provisions on the protection of e-mail, camera surveillance and the treatment of data concerning drug abuse are added to the Act.

France

The CNIL carried out 31 inspections in 2003, the most important of which concerned local authorities, credit reference agencies and debt collectors, cancer registers, controls over "cybersurveillance" activities, controls pursuant to Article 96 of the Schengen Convention. Four inspections were initiated upon specific complaints.

Other important enforcement activities concerned :

a) Fight against unsolicited faxes for advertising purposes, the CNIL having taken judicial action against eight companies in such cases.

b) Efforts vis-à-vis credit reference agencies to correct unlawful processing, with the co-operation of the supervisory authorities of the banking sector

c) Efforts vis-à-vis the "fichier PREVENTEL", a database put in place to fight against unpaid bills by the telecommunication sector.

Proactive enforcement strategies

Internal reflection is currently ongoing at the CNIL to reformulate the enforcement strategy and activities of this authority, in particular in the context of the adoption of the new Data Protection Law in France. Upon the assessment of its past enforcement activities (324 specific actions have been taken to day since the setting up of the authority in 1978), the CNIL is reflecting on a new policy which would differentiate between controls and inspections on the spot, with appropriate follow-up of complaints received, putting in place of appropriate security measures, enforcement on the Internet and even sector-based investigations, in agreement with other data protection authorities notably within the framework of the Article 29 Working Party activities.

Germany

Administrative fines were imposed in the following sectors (examples):

- Health sector: unwarranted transmission of personal data by surgeries to wrong health insurance companies (State of Bavaria: 21 fines between € 260 and 350)

- Banking sector: access to credit information (SCHUFA-Daten) of an applicant in order to use these dates for the employment procedure (State of Rheinland-Pfalz: € 2.000); careless announcement of account numbers and account balances of the co-owners of a joint account by an bank employee to another co-owner (State of Rheinland-Pfalz: € 300); unwarranted access to credit information (SCHUFA-Daten) by bank employees (State of Saarland)

- Insurance sector: acquisition by false pretences of a car owner's personal data by a car insurance company (State of Rheinland-Pfalz)

Proactive enforcement strategies (examples)

The Federal Data Protection Commissioner and the Laender authorities regularly carry out audits (more than 200 p.a.) and provide advice in the public and in the private sector. Among others, the following institutions have been audited recently: Telecommunication services, teleservice providers, health insurance companies, the Ministries of Defence, of Justice, of the Federal Employment Agency, and for Economic Cooperation and Development, various branches of local and state administration and processors.

An information brochure for citizens about data protection in the non-public area was published by the Ministry of the Interior Baden-Württemberg.

Leaflets "Bitte keine Werbung", "Handels- und Wirtschaftsauskunftsdateinen", „Videoüberwachung durch private Stellen" and "Datenschutz im Verein" were published by the Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia to inform citizens.

Greece

Further to several complaints from data subjects, fines were imposed on insurance companies for illegal data processing in the following cases:

- € 20.000 to an insurance company that refused to indemnify an insured person who underwent an operation after having access to his medical record which was kept in a medical centre without prior information of the insured person and without his consent, and € 30.000 to the medical centre for illegal transmission of sensitive data to the insurance company;

- € 50.000 to an insurance company that refused to indemnify a passenger who was wounded in a car accident after having access to a detailed report containing information about the passenger's medical and psychological background from his early years since the day of accident, which was submitted by a private investigator upon the Company's request;

- € 20.000 to an insurance company after asking an insured person, who underwent an operation, to submit a videotape of the laparotomy and the results of the histologic test in order to indemnify him.

Proactive enforcement strategies

In order to regulate situations described above, the Hellenic DPA is working on a Directive on the processing of medical data by the insurance companies.

Furthermore, the Hellenic DPA organises a plan for audits in medical centres and hospitals and in insurance companies as well.

Ireland

Because of the low level of compliance with the obligation of registration (notification) in case of holding sensitive data electronically, an awareness campaign was launched in the legal sector involving both their representative organisation and direct correspondence by the DPA to a number of legal firms. Several firms who failed to respond were inspected on-site to confirm that they had a registration requirement. Successful prosecutions of two legal firms for failure to register were taken in the District Court.

An Enforcement Notice was issued to Minister for Communications Marine and Natural Resource ordering to stop publishing personal details on their website of those that made requests for non-personal information under the Freedom of Information Act.

Investigations with regard to a number of prosecutions pending in relation to breaches of the SPAM regulations implementing Directive 2002/58 have concluded but they have not yet been heard by the court.

Proactive enforcement strategies

Audits on the Irish Data Protection Commissioner's own initiative were carried out in:

- A major hospital;

- A telecommunications company;

- An events ticket sales company;

- A financial services advisor;

- A health insurance company, and in

- A life assurance, pensions and banking organisation.

Italy

Enforcement actions are mainly based on the reaction to complaints lodged by data subjects for failure to exercise their rights (access, rectification, erasure, etc.) and on inspection/audit activities that are carried out either *ex officio* (based on an annual action plan identifying specific sectors and/or processing operations) or following complaints and reports.

Significant enforcement activities were carried out in the following sectors:

a) Biometrics

The Italian DPA stopped two initiatives by public bodies envisaging the use of fingerprint-based systems 1) for controlling access to restaurants and shops offering discounted services to low-income university students and/or scholarship recipients, and 2) for controlling presence at work of the employees at a local municipality. The Italian DPA stressed that use of biometrics-based mechanisms was disproportionate compared with the purposes to be achieved, and that specific privacy safeguards (such as enhanced security measures) were at all events necessary given the highly sensitive nature of biometric information.

b) Notification of Processing Operations

Sixteen entities, both public and private, were fined in June 2004 because they had not submitted and/or delayed submitting the notification of processing operations concerning especially sensitive data (genetic data, biometric data, health data, data concerning sex life, etc.). The inspections carried out by the Italian DPA jointly with an ad-hoc squad of the Finance Police (Guardia di Finanza) pointed out that several health care units, medical laboratories and a bank were not compliant with the newly enacted data protection Code, which considerably simplified notification requirements by making notification mandatory only in the cases specifically referred to (i.e. cases that relate to the processing of highly sensitive data and/or entail specific risks for data subjects' fundamental rights and freedoms). In addition to being fined 10,000 to 60,000 Euros, depending on the circumstances, the entities in question were banned in some cases from using the personal data in their possession, as the data protection Code prohibits use of personal data that have been processed in breach of the law.

c) Employment

Reference can be made to an issue arising frequently in the employment context, i.e. the mechanisms for accessing an employee's personal file. In two important cases, the Italian DPA found that the organisational arrangements made by the data controllers (i.e. the employers) were not in line with the security measures required under the data protection Code. In particular, a company was fined because it had allowed dissemination of sensitive data concerning an employee and her family members, whereas the information

should have remained within the employee's personal file. In another instance, a public body was ordered to adopt all the necessary security measures to prevent unauthorised staff from accessing personal files; in the case at stake, information on an employee's family circumstances had been used by other colleagues to support a complaint against that employee's allegedly unjustified leave of absence. Even though one of the said colleagues was authorised to access employees' personal files, she had used the data for personal purposes unrelated to her official duties.

Other important enforcement activities concerned the banking and telecommunications sector as well as spamming activities.

Proactive Activities

The proactive initiatives undertaken by the Italian DPA over the past years to enhance application of data protection law range from publication of a weekly newsletter to the operation of a front-office (public relation department) service and the organisation of several conferences and workshops addressing the requirements of specific sectors (health care, public administration, banking sector). Additionally, reference can be made to the adoption of several codes of conduct jointly with the relevant trade associations and categories. So far, they include the code of conduct applying to journalistic activities (adopted in 1998), processing of personal data for historical purposes (2001), processing for statistical and/or scientific research purposes within the framework of the national statistical system (2002), processing for statistical and scientific purposes (2004), and processing in connection with credit information systems (credit referencing, 2004; available in English at http://bach.drt.garanteprivacy.it/garante/doc.jsp?ID=1079077). It should be pointed out that compliance with the provisions of these codes of conduct is necessary in order for the processing of personal data in the respective sectors to be lawful and fair as required by data protection legislation.

Lithuania

During the year 2004 the Lithuanian DPA carried out 365 inspections on the lawfulness of personal data processing. 217 inspections were carried out in the public sector, 148 – in private sector. In 68 cases were imposed sanctions, in 52 cases during the inspection were eliminated the violations, in 47 cases no violations were detected. In the year 2004 were carried 37 inspections on spot.

In the year 2004 the Lithuanian DPA received 91 complaints and requests from data subjects on alleged violation of the processing of personal data. 60 received complaints are related to the private companies and natural persons. 31 complaints were related to the public sector institutions and bodies. For example, the Lithuanian DPA received 2 complaints on the processing of personal data by the General Prosecutor's Service of the Republic of Lithuania, by the Secretariat of the Chairman of the Parliament and by the Parliamentary Commission on Anticorruption. The applicants asked to find whether the General Prosecutor's Service of the Republic of Lithuania, the Secretariat of the Chairman of Parliament and Parliamentary Commission on Anticorruption processed lawfully and justly applicant's personal data. During the investigation it was detected that the Parliamentary Commission on Anticorruption was giving to press the copy of the notification on suspicion communicated excessive personal data of applicants – personal identification number, address – by not implementing appropriate organisational and technical measures designated for the protection of personal data from accidental or

unlawful disclosure. For these violations the protocol on the violations of Administrative law was issued for the Chair of Parliamentary Commission on Anticorruption and submitted to the court. The court dropped the case motivating that there had been no composition of violation of Administrative law. No violations of the Law on Legal Protection of Personal Data detected in the General Prosecutor's Service of the Republic of Lithuania, the Secretariat of the Chairman of Parliament

According to the Article 26 of the Law on Legal Protection of Personal Data there are personal data processing cases when the prior checking has to be carried out. During the year 2004 the Lithuanian DPA received 210 notification forms on prior checking. 136 notifications were investigated, 105 issued authorizations, and in 23 cases the authorization was refused. In 8 cases the investigation was cancelled. At the beginning of the year 2005 77 cases are under investigation.

In the year 2004 the Lithuanian DPA gave 1885 consultations: 1517 by telephone, 199 in Internet website, 120 in written form, 49 consultations for the media. 2/3 of given consultations were designated for the data controllers, 1/3 – for the data subjects. The specialists of the Lithuanian DPA took part in 20 TV and Radio programs. 35 press releases and 5 booklets on personal data processing issues were published.

Malta

Since its inception in 2002, the Office of the Commissioner for Data Protection has carried out inspections in the health sector and in credit referencing agencies. Notwithstanding that various complaints have been lodged by data subjects or associations representing them, the Office has not as yet imposed any administrative fines on data controllers.

Proactive Enforcement Strategy

A proactive enforcement strategy is still to be developed.

Netherlands

Further to a complaint from a data subject concerning the data processing by trade information agency "Bureau X", investigations were carried out by the Dutch DPA. Information collected by the agency seemed inappropriate for the purpose and seemingely came from illegal sources. An unannounced on-the-spot check was conducted. Due to the result of these investigations a formal complaint was filed with the public prosecutor on suspicion of fraud, enticing breach of secrecy and non-notification of the Dutch DPA. One defendant was sentenced to twelve months imprisonment. The two managers of the agency were sentenced with community service, a fine, and a suspended sentence of imprisonment Secondly "Bureau X" was threatened with financial consequences if specified proceedings were not adjusted to the satisfaction of the Dutch DPA and in accordance with the Dutch Data Protection Act. Furthermore the DPA set up a project to inform organisations that had provided information to Bureau X illegitimately of the fact that a leak existed within the organisation and urged them to undertake action to avoid such leaks. This led in several instances to changed procedures

and in some cases to discharge of employees involved in the illegitimate provision of information.

The Dutch DPA also investigates tapping of communications by police and justice.

In some instances, the threat of the use of powers sufficed, for example with regard to a case against a Dutch telecom company that had to change its information policies with regard to so-called secret phone numbers. In other cases the DPA threatened with a duty backed by an *astreinte* in order to receive the necessary information from the controllers.

Proactive enforcement strategies

The proactive enforcement strategies of the Dutch DPA will be based partly on a risk analysis model, which is currently being developed.

In 2003 and 2004 pro-active investigations were carried out to check whether and how controllers have fulfilled their notification obligation. These investigations were taken place in four sectors: municipalities, the Direct Marketing sector, health and safety executives, and health insurance companies. The DPA imposed administrative fines in several cases. The result of the notification investigation at municipalities was that it forced municipalities to straighten out their personal information systems and processing. It also led to peaks in notifications.

The Dutch DPA also conducted on the spot investigations at the Criminal Intelligence Units. Furthermore, after having approved certain black lists in the banking sector by means of a prior checking, the Dutch authority decided to control the implementation of the black lists in practice.

Poland

The Inspector General for Personal Data Protection attaches a special significance to inspection activities as a good source of information and the opportunity to make verification of information provided by the controllers within the course of registration and complaint proceedings. These inspection activities are being carried out on the spot, in the controller's seat by very well qualified employers of the Inspector General. The inspection team includes both lawyers and IT experts who cooperate with each other in carrying out the inspection activities. According to the Bureau's statistical data – 142 inspections has been carried out in 2004.

Inspections were performed in the following sectors:

- Public sector (including courts, public prosecutor's offices and revenue offices);
- Financial sector (including banking sector);
- Insurance sector;
- Telecommunication sector; and
- Marketing sector.

For example, in one of the cases the Polish DPA stated that on a Website administered by X company, materials are published according to which upon concluding contracts on the provision of telecommunications services within Y Network, the X company collects personal data of these persons by making Xerox copies of specific documents, in particular ID cards on which photos of their owners are placed. Considering the fact that making Xerox copies of ID cards by the company may lead to the collection of users' personal data in the scope wider than allowed by law, i.e. in scope of image and description, the DPA instituted ex officio proceedings in this case and in its course addressed a request to the company for submitting explanations. In the end the DPA ordered by means of an administrative decision the blocking of the processing of the data indicated above.

Inspection activities in the pharmaceutical sector are planned for the next year.

Proactive enforcement strategies

The sectors described above (public, financial, banking, insurance, telecommunications and the marketing sector) are crucial from the perspective of possible enforcement activities plans.

Spain

In the private sphere the Spanish DPA carried out investigative actions and imposed penalties mainly in the health sector and telecommunication sector (examples):

- The most common problems in the health sector are related to security measures required and to the duty of secrecy concerning information relating to individuals' health. In the case of security clinical information was found in rubbish bins. A serious violation of the duty of secrecy in the processing of medical data is the case of giving a family member the results of tests carried out on a patient, without the patient's consent. Another problem that is leading to a significant number of claims in the health area is the processing of employees' data. There was also one case relating to the processing of health data in the insurance industry. Another case dealt with the assignment of data between insurance and reinsurance companies.

- The most significant problem that has been raised in the telecommunications industry is related to the fraudulent pre-assignment of telephone lines without the knowledge or consent of the person concerned. When the subscriber receives the invoice he refuses to pay it because he has not contracted it from the operator concerned. The final result of this practice can be the subscriber's inclusion in an information file on his personal assets and creditworthiness; because he has not paid the debt. Numerous claims have been made to the Spanish DPA by people affected by this situation, which has been declared an offence contravening sections 6 and, if applicable, 4.3 of the Spanish Data Protection Act, the telecommunications operators being declared liable. Subsequently proceedings have also been taken against the distributors who provide the information needed for activating the pre-assigned service. Another problem in the telecommunication sector is the unwanted advertising. A decision concerning an unsolicited direct sales call, using automatic call services, declared that an

offence had been committed because it could not be shown that the person affected had given his consent.

Also in the public sphere the Spanish DPA carried out investigative actions and imposed penalties (examples):

- Relating to the data processing in health institutions in proceedings not only a breach of security measures was found. There was also a case where a patient's clinical information had been used by an employee of a health centre for private purposes. In this case, the data controller was asked to initiate disciplinary proceedings against the employee concerned.

- In the case of processing data relating to individuals' working lives, in 2003 four decisions have been given in cases in which users authorised to access such information used it for private purposes unrelated with the duties that justified access. In all these cases the introduction of security measures and the collaboration by the Social Security Authorities enabled the unlawful processing of personal data to be detected. It was asked for disciplinary actions as well.

The Spanish DPA also carried out actions to safeguard citizens' rights (access, rectification and deletion) that did not involve penalties, and which were limited to accepting or rejecting claims made by the public to the DPA.

Proactive enforcement strategies

Inspections took place within the project "2001 Census of Population and Housing" that is carried out by the National Institute of Statistics over a period of several years, and in which other public bodies and private companies are collaborated. The investigations by the Spanish DPA, which looked in particular at the provision of services involving the automated processing of personal data, were undertaken in two phases between June 2001 and December 2002, in which 35 procedures were carried out in the installations of 14 companies and various offices of the National Institute of Statistics. Recommendations were issued that emphasise the prerequisites that should be included in contracts for the lawful conduct of subcontracted companies when they are not acting on behalf of the controller of the file.

An inspection plan was also implemented for hotel chains, in order to determine the extent to which their files meet the requirements of the Spanish Data Protection Act and its subsidiary legislation. In 2004 recommendations will be issued that will set out the legal criteria required in applying the data protection legislation.

Sweden

Inspections were carried out in local social administration and local environmental administration. It was found that in many cases information to the data subjects was insufficient and that there were insufficient routines regarding the right of access on request from the data subject, deletion of data and the checking of access to data. After having informed controllers during inspections about what they needed to rectify, inspections were closed.

A similar project has been carried out regarding personal data processing in connection with collection and storage of biological samples. In some cases, there was some uncertainty as to whom should be regarded as the personal data controller. The Swedish DPA found it necessary to provide information about, for example, the rules on information to data subjects, on consent and on third country transfers.

The Swedish DPA has also carried out other supervisory activity following complaints from individuals regarding for example processing of personal data on websites without consent and processing of data for direct marketing purposes regarding individuals who have opposed such marketing.

Proactive enforcement strategies

The Swedish DPA decides on different supervisory projects for each year. Inspections in local administrations referred to above are examples of such projects which are proactive in the way that the results are gathered and published in reports that are distributed to other controllers in the same sector.

United Kingdom

Enforcement actions include direct marketing and the unfair processing of personal information by recently privatised utility companies and companies sending unsolicited mail. Also credit reference agencies were targeted on the basis that they were processing personal information unfairly and for incompatible purposes. Enforcement actions have been carried out in the public sector including action against police forces in respect of conviction data held on the Police National Computer and also in respect of the Prison Service concerning systematic failures to provide subject access.

Proactive enforcement strategy

A proactive enforcement strategy is presently work in progress.