Review of 2003

Although the right to protection of privacy is a constitutional right, this does not make it an absolute right. This right entails handling personal data with proper respect and caution. Vested in this are interests that will require constant balancing against other interests. In the public sector, this weighing up of interests is ultimately reviewed in parliament and is usually translated into guarantees for citizens with regard to collecting and using their personal data. Citizens usually have no objections to this assessment. Both sides of the balance are after all weighted by authentic interests. However, the rights of citizens in a democratic state of law are not served if government bodies deal with their personal data arbitrarily. A democratic balancing of interests should result in the careful, systematic government processing of citizens' personal data. The Dutch Data Protection Authority (DPA) is concerned about the erosion in public debate of the fundamental principle laid down in international treaties that the use of personal data and violation of personally privacy should be an actual necessity.

Privacy and security
Although the right to protection of privacy is a constitutional right, this does not make it an absolute right. This right entails handling personal data with proper respect and care. Vested in this are interests that will require constant balancing against other interests. In the public sector, this weighing up of interests is ultimately reviewed in parliament and is usually translated into guarantees for citizens with regard to collecting and using their personal data. Citizens usually have no objections to this assessment. Both sides of the balance are after all weighted by authentic interests. The interests of citizens in a democratic state of law are not served if government bodies deal with their personal data arbitrarily. A democratic balancing of interests should result in the careful, systematic government processing of citizens' personal data. The Dutch Data Protection Authority (DPA) is concerned about the erosion in public debate of the fundamental principle laid down in international treaties that the use of personal data and violation of personally privacy should be an actual necessity.

Necessity as guiding principle

The necessity principle is eroded when politicians, civil servants and policy makers no longer ask whether gathering, using and retaining citizens' data is necessary for a specific purpose. The fact that institutions dispose over considerable quantities of citizens' details does not automatically legitimize using these data for other purposes, nor retaining them for extended periods or sharing them with other organisations.

The criteria of necessity leave scope for the use of a basic set of citizens' data by various government bodies and related agencies. Also collaboration between institutions is very well possible, providing organisations continually monitor which exchange of information is required for the collaboration, and providing the citizen in question is properly notified. The distribution of duties between public-private bodies creates a more complex situation. The transfer or contracting out of social security components calls for paying close attention to the correct use of (generally highly specific) personal data by the market parties. Contracting out activities does not acquit the government from its responsibility for ensuring that personal data are treated with due care.

Monitoring, security and freedom

Public debate constantly resounds with the call for more monitoring measures. Objective weighing up and realistic assessment of the effect of proposed measures seem to cave in beneath the very real threat of terrorist attacks and the problem of serious forms of crime. The symbolism of the proposals often is, however, far greater than their efficiency. Increasingly far-reaching monitoring measures will however not necessarily result in increasing citizens' security, while the social burden for state and citizens is considerable. Paying too much attention to security will encroach upon the freedom of the citizen in the long term.

Reflecting on the purpose, necessity and scale of monitoring measures to be taken, is imperative. Measures could also be temporary; their scope can be limited to places or times where there is increased risk. Evaluating the measures should be standard practice, certainly in the case of radical monitoring means like surveillance cameras, preventive searching and identity checks. Well thought out measures, their proportional use and measuring their efficacy in combating terrorism and other forms of serious crime are part and parcel of a government that protects our constitutional rights.

Privacy from the outset

When the new cabinet was installed in 2003, the Dutch DPA asked that attention be paid to the issue of processing personal data with due care. On a number of points – health care, security, tackling fraud and electronic government services – cabinet policy does after all touch on the careful and lawful processing of personal data. If privacy protection is disregarded, the ability of policy initiatives and government action to stand up in court can be at considerable risk. There is greater scope for success by paying close attention to privacy protection from the outset, when designing measures and information systems.

Legislative proposals that largely relate to processing personal data should be submitted to the Dutch DPA for advice. In consultation with the ministries, better conditions for fulfilling this obligation were created in 2003.

Information infrastructure

Streamlining basic data should not end in the unbridled flow of personal data within the government. A specific and clear legislative rule is required to cover large data flows, with attention for such aspects as social necessity, distribution of tasks and roles, actual data traffic and transparency.

In 2003 the recommendations of the Persoonsnummerbeleid (Personal Identification Number Policy) of the Tafel van Thijn (the Van Thijn Committee) on setting up an umbrella information infrastructure for the government, was followed up. The Dutch DPA was intensively involved, both at steering group and working group level, in developing a plan for the introduction. Among other things, the Dutch DPA contributed to the proposals for a Nationale Vertrouwensfunctie (National Confidentiality Function), an organisation that will be charged with providing citizens with insight in all data flows on the basis of the burgerservicenummer (public service number). Citizens' confidence in the electronic state is essential. This is why the Dutch DPA will recieve the means to examine current and new data processing and fulfil the role of 'ombudsman' in this area in future.

Municipalities

For the citizen, the municipality is an important area of government with which he or

Results secured in 2003

IN THE PREVIOUS ANNUAL REPORT, IT WAS ANNOUNCED THAT IN 2003 OUR TARGETS WOULD BE AS FOLLOWS:

- **Advice on legislation**
  In accordance with Article 51, second paragraph of the Personal Data Protection Act (WBP), the Dutch Data Protection Authority (DPA) should be asked to provide advice with regard to legislative proposals and the drawing up of implementing regulations (AMvBs) with any degree of relevance to the processing of personal data. The Dutch DPA has asked nearly all the Ministries to pay heed to the obligation to request for advice and has managed to make agreements in order to adequately fulfil this requirement.

- **Data protection officers**
  By the end of 2003, another 51 officers charged with data protection had been reported to the Dutch DPA on the grounds of Articles 62-64 of the Personal Data Protection Act, bringing the total number to 148. The Dutch DPA helped to organise a contact day for data protection officers employed by municipal authorities and all officers have been allocated a contact person within the Dutch DPA. The working relationship between the supervisor and the data protection officers is still being developed.

- **Camera surveillance**
  In 2003, the Dutch DPA published the results of a survey on the operation of camera surveillance of public places in Dutch towns and cities and how the various municipal authorities treat the privacy aspects. The report was entitled *'Cameratoezicht in de openbare ruimte. Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten'* (Camera surveillance of public places. Investigation into the use of camera surveillance in all Dutch municipalities).

- **Sick employees**
  For many years, attempts have made to stem the flow of sick employees claiming disability benefit under the Disability Benefits Act (WAO). This has led to an increased need for information on sick employees, thereby directly affecting the privacy of said employees. In 2003, the Dutch DPA completed an investigation into the privacy aspects of the complex rules and regulations and the main flows of information regarding sick employees. Publication of this investigation has been delayed.

- **Police registers**
  Following up on previous activities concerning the registers of the Criminal Intelligence Service Units (CIEs), the Dutch DPA has started a random investigation of the practices of eight of these units. The selected dossiers were examined to determine the extent to which the regulations governing data processing were actually being observed. The investigation is due to be completed in 2004.

- **Telecommunication**
  The Dutch DPA has been looking into notification obligations within the telecommunications sector and has been providing advice with regard to the new Telecommunications Act. In late 2003, the Dutch DPA consulted the sector in writing on the issue of number identification with a view to clarifying the standards used in practical situations.

she will be greatly involved. As a result, municipalities process great quantities of citizens' personal data. Because of developments in the duties and administration of the municipality, responsibility for protecting personal data is increasing. Consequently, it is crucial that municipalities have their information systems well organised, also with a view to protecting the personal data of their citizens.

An analysis of the first 13,000 notifications of processing personal data under the Wet bescherming persoonsgegevens (Personal Data Protection Act) showed that the number of notifications from municipalities greatly lagged behind expectations; at least 60 municipalities appeared to consistently ignore their obligation to notify. In a random check the Dutch DPA then assessed a number of municipalities to see whether they had complied with the obligation to notify. In December 2003, the first municipality was penalised for failing to comply with this obligation.

Public camera surveillance

In 2003 the Dutch DPA commissioned a survey into the use of camera surveillance by municipalities. The goal of the survey *Cameratoezicht in de openbare ruimte* (camera surveillance of public places) was to gain an overview of the way in which CCTV surveillance functions in practice and how the various municipalities address the privacy aspects of camera surveillance. The survey showed that one in five municipalities de-

- **Certification**
  The results of a previous project entitled 'Auditaanpak' (Audit Approach) have been used as the basis for developing a privacy certification scheme. The aim of this scheme is to comply with the legislation on privacy by further advancing self-regulation. In 2003, the Dutch DPA, in partnership with the future accreditation institutions NOREA *(National Professional Association for IT Editors in the Netherlands)* and the NIVRA *(Royal Netherlands Institute of Registered Accountants)*, ensured that this scheme was almost ready to be put into operation.

- **Notification obligation**
  The obligation to notify the processing of personal data to the Dutch DPA contributes towards transparency and enables verification and supervision. In 2003, the Dutch DPA used the public register to carry out an analysis of notifications with a view to the enforcement of this obligation. More detailed investigations were eventually conducted into three sectors and the municipal authorities which led to the first administrative fines being imposed in late 2003.

- **Internet site**
  Access to the Dutch DPA web site has been improved. Amongst other things, theme dossiers and an e-mail newsletter have been introduced. The increasing size of the web site and the need to provide insight into policy regarding new Dutch DPA tasks meant that in 2003, a start was made on re-designing the Dutch DPA web site. The planned separate section for dealing with practical questions from data subjects has not been realised. This will now be included in the new design.

- **Organisational set-up**
  In order to ensure that the new tasks in the areas of supervision and enforcement are carried out satisfactorily, the Dutch DPA has made modifications to its organisational set-up. In line with this new organisational set-up, the Intervention, Objections and Appeals Department has been operating since 1 January 2003. The modernisation of the organisational structure was rounded off in 2003 by the instigation of the Investigations Department on 1 January 2004. In as far as this was possible, the job profiles accompanying these changes were realised in 2003.

ploys such surveillance as a means of furthering security, public order and supervision. Over half of the municipalities that make use of CCTV however, have not reviewed its effectiveness. Around half of the municipalities use camera surveillance in the context of cooperation between institutions and organisations. This generally involves cooperation with the police in tracking down criminals, although cooperating with companies and other organisations is also a regular occurrence. The frameworks within which this takes place, however, often seem unclear.

Rotterdam: a personal approach is possible

At the end of 2002, the Dutch DPA contested the view of Rotterdam city council that adjusting privacy legislation was necessary for a safe city. Following on from this, in 2003 the Dutch DPA consulted all the parties involved in the various projects for an integral approach to around 700 drug addicts causing public nuisance, committing crimes and also avoiding medical and welfare aid. The police, welfare bodies and the probation service all took part in this project. Data on the contacts of addicts with police and the welfare authorities was exchanged. The shared information is stored in a basic dossier. The specific approach to be adopted, consisting of various forms of voluntary and compulsory treatment programmes, is then determined on the basis of the dossier.

Discussions with the partners in the project focused on the limits circumscribed by care workers' professional confidentiality. In the consultations, the Dutch DPA pointed out that welfare workers should adhere to their statutory duty of acting in the client's best interests. If, in their professional opinion, sharing information on the client with other bodies is in the client's best interests, it is possible in principle. This approach prompted a wider debate on the scope of medical professional confidentiality under the direction of the Inspectie voor de Gezondheidszorg (Health Protection Inspectorate). In the course of 2003, the parties involved elaborated the rules governing information exchange and the Informatiesysteem PGA (PGA Information System) was notified to the Dutch DPA.

Insufficient supervision of the implementation of the WWB

The core of the new Wet werk en bijstand (WWB or Work and Income Act) determines that municipalities acquire more (financial) responsibility for social security. In 2002 and 2003 the Dutch DPA drew attention to the system of supervising the implementation of the WWB. There is a gap between the official rule that the *Inspectie Werk en Inkomen* (IWI or Work and Income Inspectorate) supervises the legitimacy of implementation (including processing data on individuals) and the practical detailing in which the IWI does not receive the information necessary for structurally exercising supervision. This gulf has not been bridged during the discussion of the bill in both Houses. As regards processing (personal) data, the elaboration of the supervision is not in line with the view of the Dutch deputy minister of Social Affairs and Employment expressed during the parliamentary discussion. The Dutch DPA is concerned about the municipalities' lack of a duty to give account.

Police and privacy

The contribution of a number of chiefs of police to the public debate on security was out of balance. Protection of privacy was repeatedly underlined as an obstacle to police work, a hindrance to achieving better results. Prominent police officers seemed to deny the fact that the police has recourse to an extremely diverse range of sources of infor-

mation about citizens. With this, privacy protection obligates the police to deal with data in a responsible, controllable manner. The Groningen chief of police's typification of the constitutional right to privacy as a 'refuge of evil' was way out of line.

The Dutch DPA acknowledges that the police have a considerable and legitimate need for information and agreed with the main points laid down in the planned expansion of the powers of the Ministry of Justice and police to request personal data from organisations and companies, if necessary to an investigation. The bill is based on proposals tabled by the Mevis committee (2001) and primarily creates clarity for the business sector. The Dutch DPA is of the opinion that a counterweight is required. Information should not only be gathered and used purposively and selectively but police information administration must be supervised by, among other things, periodical and independent retroactive checks. In the cabinet standpoint on the proposals of the Mevis committee, the Minister of Justice also promised to effectuate this. The Dutch DPA insisted on the speedy implementation of these periodical audits on all police registers.

Criminal Intelligence Service Units

In 2003 the Dutch DPA commenced an initial series of audits into the criminele inlichtingen eenheden (CIEs or Criminal Intelligence Service Units) of eight police forces supplementary to the self-evaluation and independent review organised by the police in 2002. CIEs maintain a number of exceptional registers that also contain investigative data on persons who are not suspected of criminal involvement. Independent, external supervision is therefore of essential importance. Only the Dutch DPA can, as an external supervisor, appraise itself of the content of the dossiers. This series of surveys involved carrying out spot checks to audit this practice. In the selected dossiers, the research assessed the degree to which the rules for processing information were actually followed. The audit round will be completed in 2004.

Lawyers tapped

The Dutch DPA investigation into listening in on and registering conversations between citizens and their lawyers showed that there was insufficient respect for lawyers' professional confidentiality. The systematic recording, registration, working out and examination of this confidential communication by the police and *Openbaar Ministerie* (OM or Public Prosecutors Office) is in conflict with the exceptional position of those who can claim professional confidentiality as acknowledged in legislation and treaties. Consequently it is also in conflict with the *Wet politieregisters* (Police Registers Act) and the *Wet bescherming persoonsgegevens* (Personal Data Protection Act). Police and justice had gone too far in listening into and recording conversations between citizens and their counsel. The Minister of Justice did not however share the Dutch DPA's views on this, and did not adopt the recommendations.

Reducing the administrative burden

The number of requests submitted to the police by individuals wishing to know if and how they are registered in police registers, showed a considerable upswing in previous years. The number of requests jumped from 1100 in 2000 to 1850 in 2002. They primarily concerned complex, labour-intensive requests from lawyers, which were dealt with by a CIE. A working group of privacy experts from the police, the OM and the Dutch DPA devised a plan to streamline handling the requests. This will also prevent the erosion of

the right of inspection.

In the context of reducing the administrative burden, the model regulations for police registers are also important. In 2002, the Dutch DPA approved 40 model regulations for the permanent registers. In 2003, the *Modelreglement Tijdelijk Register* (Temporary Register Model Regulation) came into force. The use of model regulations immediately reduces the administrative burden for police and the Dutch DPA and simultaneously creates safeguards.

Market mechanisms in the healthcare sector

The discussion on cost control and improving quality in the healthcare sector is supported by a consensus on the need for stimulating market forces through public-private cooperation while an extremely prominent role for the healthcare insurance companies is beginning to take shape. However, the insurance companies assert that they cannot fulfil this role without maximum insight in the actual, individual healthcare cases. This emerged in the discussion on the introduction of the *Diagnose Behandeling Combinatie* (DBC or Diagnosis-Treatment Combination).

The DBC system was developed to defray the costs of specialised medical care and should result in a price development that conforms to the market on the basis of negotiations between healthcare institutions and medical insurance companies. A DBC is a combination of codes that contain data on, among other things, the demand for healthcare, the diagnosis and the treatment of a patient. This information is covered by the code of professional medical confidentiality. Healthcare professionals are expected to provide the DBCs to insurance companies as an account of the care provided.

The Dutch DPA emphasized the importance of professional medical confidentiality and proportionality in furnishing personal medical data. The Dutch DPA insisted that there should be greater clarity surrounding the personal data that hospitals are required to provide to health insurance companies. Once the data processing necessarily required for various legitimate purposes has been clarified, the legal embedding of the new pay system could be tailored to match it. Working out this necessity requirement resulted in a checking framework. This offers five criteria which serve as a basis for determining whether a DBC can be declared or not, together with all corresponding data on the diagnosis.

The DBC system will be gradually introduced starting on 1 January 2005. In a joint letter, the Minister of Health, Welfare and Sport and the Dutch DPA asked the parties involved (such as *Zorgverzekeraars Nederland* and professional associations) to bring the method involved in introducing the system to the attention of their members.

Sick employees

For several years now, attempts have been made to limit the number of sick employees claiming disability benefits under the Wet op de Arbeidsongeschiktheidsverzekering (WAO or Disability Benefits Act). This led to measures for a more active sick leave policy, more stringent reintegration obligations for employee and employer and a longer obligation for employers to continue paying wages. Further, other organisations and companies have also become involved in the system. All these parties have an increasing need of information on the sick employee, which directly impinges on his or her privacy.

Given the complexity of the legislation, in 2002 the Dutch DPA launched a study of the most important data flows concerning sick employees and the corresponding privacy

regulations. The study was rounded off in 2003. Once more, the importance of clear legislation on public-private cooperation was undeniable. More than government bodies, companies have an interest in clarity on what is and is not permitted, both in terms of management and reputation and liability.

Certification of data processing

In various countries a search is being conducted into ways of utilising competition and market mechanisms for privacy protection. One of the options of making it clear in the market that companies and organisations endeavour to handle personal data with due respect and care, is a privacy certificate. Together with the Dutch DPA, a number of regulatory bodies have developed a system for the private auditing of processing personal data. The privacy certificate in mind can be allocated to a specific, legitimate processing of personal data. The certificate is thus not awarded to an organisation in its entirety. In the first instance, the Dutch DPA will appoint two accreditation bodies, the NOREA and the NIVRA for the accreditation of privacy auditors. The system will gain practical form in 2004.

Codes of conduct for the business sector

When protecting personal data, explicit scope has been created for self-regulation by, among other things, codes of conduct that have been approved by the supervisor. Codes of conduct are important because the specific working out of privacy norms for a sector or profession creates clarity for professional practice. The Dutch DPA was involved with the realisation of codes of conduct for financial institutions, the bailiffs and the first European code of conduct for direct marketing.

The Privacygedragscode sector particuliere onderzoeksbureaus (Privacy Code of Conduct for Private Investigation Agencies) approved at the beginning of 2004 was drafted by the *Vereniging van particuliere Beveiligingsbureaus* (VPB or Association of Private Security Agencies) and binds the agencies affiliated to the VPB. Private investigation is a sector experiencing exponential growth, and one in which little was regulated. In the context of licensing these agencies, the Minister of Justice is planning to obligate all private investigation firms to comply with this code of conduct. The Minister of Justice and the Dutch DPA have concluded an agreement to coordinate supervision of the branch.

The Code of Conduct for processing personal data of the *Nederlandse Vereniging van Handelsinformatiebureaus* (NVH or Netherlands Association of Business Information Agencies) was also approved. In this sector in particular, over the last few years, the Dutch DPA was forced to conclude that personal data protection was not properly observed on a large scale. The Dutch DPA will maintain the code of conduct of the NVH as a guideline in supervising all trade information bureaux.

Penalty for business information bureau X

In 2003, the Dutch DPA published the results of the investigation into business information agency X. The conclusion was that the bureau had processed personal data illegitimately, improperly and negligently when compiling reports of claim information. The Public Prosecutor was informed that the company was suspected of having committed a number of punishable offences. The criminal investigation has since resulted in the prosecution and trial of a number of individuals involved in the enterprise.

Targets for 2004

THE MAIN TARGETS FOR 2004 WILL BE AS FOLLOWS:

- **Sick employees**
  The investigation of the most important data flows with regard to sick employees and the relevant privacy regulations will result in a study being published in 2004 containing rules of thumb to be used in the practical situation. This study will be brought to the attention of the various parties involved in the reintegration of sick employees.

- **Police registers**
  The investigation that was started in 2003 into the registers kept by the Criminal Intelligence Service Units at eight regional police forces will be completed in 2004. The general findings of this investigation will be published.

- **Investigation of wiretapping rooms**
  In 2004, the Dutch Data Protection Authority (DPA) is to conduct an investigation into the privacy aspects of data processing in police wiretapping rooms, as a follow-up to the 2003 investigation into the safeguarding of confidential communication between lawyers during the interception of telecommunications *(Onderzoek naar de waarborging van de vertrouwelijke communicatie van advocaten bij de interceptie van telecommunicatie)*.

- **Camera surveillance**
  The results of the investigation published in 2003 entitled *Cameratoezicht in de openbare ruimte. Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten* (Camera surveillance of public places. Investigation into the use of camera surveillance in all Dutch municipalities) will be used in 2004 for a study of the privacy aspects of camera surveillance of public places, which will outline rules of thumb for practical situations.

- **Public service number**
  The Dutch DPA will make a contribution towards the realisation of the *Nationale Vertrouwensfunctie* (National Confidentiality Function), an organisation which has been given the task of providing citizens with insight into the various data flows on the basis of a *burgerservicenummer* (public service number). During 2004, the Dutch DPA will be given the chance to start assessing existing and new data processing methods and to prepare for a future watchdog function.

- **Certification**
  The scheme developed in collaboration with the NOREA *(National Professional Association for IT Editors in the Netherlands)* and the NIVRA *(Royal Netherlands Institute of Registered Accountants)* for privacy certification is due to be put into operation in 2004. It will initially take the form test certifications, but will later become a market product. The Dutch DPA will help to assess the process of test certification.

- **Introduction of DBC system**
  In the area of healthcare, the Dutch DPA will closely follow the development and introduction of the health care finance system based on the Diagnose Behandeling Combinatie (Diagnosis-Treatment Combination).

- **National registration systems in the healthcare sector**
  In 2003, the Dutch DPA completed an exploratory investigation into five national registration systems in the healthcare sector. In 2004, the Dutch DPA will use the results of this investigation to formulate standards for use in national registration systems and the related enforcement policy.

- **Investigation into perception of privacy**
  The Dutch DPA is to conduct an initial enquiry into aspects of Dutch citizens' perception of and need for privacy. Investigations of this kind have already been carried out in various other European countries. The findings will be used to help make strategic choices and to formulate the policy of the supervisory body.

- **Policy regulations and 2nd line position**
  The Dutch DPA is to publish policy regulations for dealing with cases and the publicity surrounding them. In order to attain a 2nd line position, the Dutch DPA will approach sector, branch, umbrella and professional organisations to explore the possibility of exchanging information and dividing the tasks involved in providing information and handling complaints.

- **Organisational development**
  The Investigations Department is to become operational in 2004, focusing on the differentiation of the various forms of investigation and the development of risk analysis as an instrument for devising policy. The department will play an important part in the planned investigation into the perception of privacy and is responsible for the analysis of notifications for 2004.

- **Dutch DPA web site**
  The Dutch DPA is to revamp its web site in 2004 with a view to providing better information to data controllers and data subjects. Publication of information material on the web site will be more geared towards FAQs. This should result in a reduction in the annual flow of requests the Dutch DPA receives for information by telephone, e-mail and in the post.

The Dutch DPA had concluded that the bureau had illegitimately gathered personal data from all kinds of sources – including the tax administration, social security and benefits agencies and housing cooperations. Subsequently the Dutch DPA informed a large number of these bodies, companies and professional associations of the findings of the investigations so that they were able to take suitable steps. To which purpose, a number of organisations received relevant sections of the material serving as evidence.

In May 2003, the Dutch DPA imposed an obligation on bureau X subject to a penalty in case of non-compliance. The sanction focused on compliance with two points on which breaches of the WBP had been concluded: bureau X must refrain from processing personal data covered by professional confidentiality or which are banned from being processed, and the bureau must inform the individuals on whom it has gathered personal data.

Properly informing clients

In principle, companies have considerable options for processing personal data for market purposes. A key condition for the legitimate processing of information, is to furnish clients whose data is involved, with good information. Transparency is also essential for maintaining customer confidence. This re-surfaced in two issues: the unlisted number policy of the Dutch telecom company KPN and the creation of a central database for client data at the ING Group.

The ING Bank, Postbank and RVS (all parts of the ING Group) had sent a letter to their clients in 2002 outlining the plan to store their data in a single central system in future, for marketing purposes. The information offered, however, gave clients insufficient chance to exercise their rights. After an investigation, the Dutch DPA arrived at the conclusion that the companies had acted wrongfully. Because of the lack of specific detail in the letter sent to the data subjects, i.e. the clients, on the provision of data, the data provision was not compatible with the purpose for which the data had been gathered. The ING Group should have given the clients of the various sections clearer information in order to be permitted to further process their data at central level. The clients of ING Bank, the Postbank and RVS subsequently received additional information.

In mid 2003, the Dutch DPA and the OPTA (Independent Post and Telecommunications Authority) published an investigative report on the policy of Koninklijke KPN N.V. (KPN) on so-called ‘secret numbers’ (unlisted numbers). In the mid-nineties, KPN seems to have altered its policy, and has for some time been passing on addresses of subscribers with unlisted numbers to third parties for direct marketing purposes, without having explicitly informed its subscribers to this effect. The Dutch DPA requested KPN to actively inform its clients on the secret numbers policy. It is disappointing that the issue dragged on into early 2004 despite that fact that it essentially concerns a company’s statutory obligation to inform clients of their statutory rights.