Review of 2004

The bombings in Madrid and the murder of Theo van Gogh have resulted in an intensification of the pursuit of a safe society and in particular of the fight against terrorism. In short order a number of extensions to the powers of the police and the Ministry of Justice were implemented or announced, which will result in more and more information on citizens who are not suspects ending up in police files. For years there have been calls for extended powers, but the increased threat of terrorism since September 11, 2001 has made way for a conviction that such an extension is in fact necessary.

Needless to say, the Dutch DPA (Dutch Data Protection Authority) supports the need for the Government to take effective measures to combat terrorism. However, international treaties, European rules, the Dutch Constitution and other laws demand that new powers meet the joint criterion of usefulness and necessity. Legal protection must also be provided for. It may be necessary to venture out in different directions in the battle against the new terrorism, but there is no reason to give up the view that exercise of power and law enforcement must take place within a system of checks and balances: no powers without demonstrable necessity and no powers without the use of these powers being monitored.

Terrorism and safety

Combating terrorism

In their 'terrorism' memorandum to the Lower House on 10 September 2004, the Minister of Justice and the Minister of the Interior and Kingdom Relations announced new methods and powers for combating terrorism. Among other things, the Government envisaged comprehensive collection, linking and analysis of information about groups and persons as the key to preventing terrorism. For this purpose, the Government deemed an extension to detection powers to be necessary. It announced it would reduce the legal criterion – 'suspicion or reasonable suspicion of involvement' – for the authorisation of such actions as tapping telephones, monitoring Internet use and surveillance to 'indications of involvement'. The information exchange between security services, the police, the Public Prosecution Service and the IND (Immigration and Nationalisation Service) was to be intensified by means of an information hub, the Counter-terrorism info box, where files would be combined and analysed. According to the Ministers' memorandum, for the Government the mere fact that a citizen acts suspiciously is sufficient reason to put him under surveillance to assess whether the suspicion is justified or not.

In a public response to the proposals the Dutch DPA came to the conclusion that the necessity for an expansion of the powers to collect information had not been demonstrated. The new powers would be an addition to the anti-terrorism legislation that came into effect on 1 September 2004. The scope of the Criminal Code was expanded with new penalisations and through increasing the sentences for criminal offences with terrorist objectives. Conspiracy (in other words making arrangements) to commit terrorist acts also became a criminal offence. No experience has yet been gained with these new legal stipulations for information processing that provides an insight into the usefulness and necessity of the proposed measures. Added to this there are the recently implemented or yet to be implemented powers to intercept telecommunications and the power to request information from companies and other organisations.

Furthermore, the proposed far-reaching coordination of the gathering of information fails to recognise the separate legal responsibilities and powers of intelligence services and the police. Protecting the security of the state is primarily the business of the intelligence services. These services have far-reaching powers to collect information at the merest hint of suspicion that the security of the state is at risk. The police can only receive information from, particularly, the General Intelligence and Security Service if this aids them in their performance of police duties. The Dutch DPA therefore issued a warning against a development whereby information on a lot of citizens who are not suspects would leave the files of the security services to end up in the police files.

The proposed plans also lacked a proposal for the adequate and structural control of the process of collecting and sharing information. It would be a serious shortcoming if the Government did not provide for this control. A lot of the work carried out would remain hidden, also to persons who were the unjustified subject of an investigation. It is therefore all the more necessary to build in controls for the exertion of these far-reaching Government powers. Citizens must be protected against terrorism, but must also be able to have confidence that the Government will exercise its far-reaching powers legitimately.

In 2005, meanwhile, the Dutch DPA has further defined its standpoint in the advice on the draft legislative proposal regarding special detection powers to track terrorist activities. The Dutch DPA has not received any further information from the Ministers in question regarding the CT info box. The Minister of Justice has promised the Lower House to provide further written information on this subject.

Telecommunication records

The ongoing Europe-wide debate about a duty to retain telecommunication records for the purpose of criminal detection was given a new slant in the aftermath of the terrorist attacks in Madrid. As a result, the European Council adopted the Declaration on Combating Terrorism on 25 March 2004. This Declaration called for proposals for a mandatory traffic data retention for providers of telecommunication services. The Dutch DPA responded to this call and made a substantial contribution to the advice issued by the Article 29 Working Party – the collaboration of privacy regulators in the EU – in respect of the duty to retain records, which was also submitted to the relevant Standing Committees in the Upper and Lower House. Building on earlier opinions issued since the Nineties and decisions made by the European Court of Justice, the Working Party formulated the opinion that the proposals for a mandatory traffic data retention with regard to all telecommunication contravene the stipulations of Article 8 of the European Convention on Human Right (ECHR): no necessity for the long-term retention of all telecommunications traffic data of persons who are not suspects has been demonstrated. Such systematic storage of information is disproportional.

Passenger data

In the opinion of the Article 29 Working Party the outcome of the negotiations between the European Commission and the United States regarding the transfer of passenger data to the US remained below par on a number of points. Nonetheless, the European Commission has made a positive decision in respect of the level of protection in the US. The European Parliament brought the matter before the European Court.

The Article 29 Working Party subsequently focused on the proper implementation of the final decisions. To this effect a model was created for the provision of information to passengers. The airlines were consulted about the provision of information to passengers. The Working Party also urged the earliest possible transition from pull to push, in other words, from opening up the reservation system to the American authorities so that they can collect the information required, to the active supply of the necessary data by the companies themselves.

Duty of identification

Early in 2004 the Dutch DPA advised the Minister of Justice against submitting the legislative proposal on the expansion of the duty of identification. The main argument for this advice was that the legislative proposal created a general duty of identification for citizens, both to the police and to other supervisory authorities. However, the legislator did not sufficiently substantiate and justify such a duty of identification.

Only relatively few years ago the Kok Government concluded that a general duty of identification would be going too far. The clarification with the legislative proposal did not raise any new arguments and the Government therefore failed to meet the requirement in Article 8, paragraph 2, of the ECHR, which stipulates that infringements

Results secured in 2004

WITH REGARD TO THE OBJECTIVES SET FOR 2004 THE FOLLOWING RESULTS HAVE BEEN ACHIEVED:

- **Employee illness**
  In May 2004 the investigation into the main data flows in relation to employee illness and the associated privacy rules resulted in the publication of a reference work with practical rules of thumb: *Employee illness and privacy - rules for the processing of data on sick employees.* The reference work was brought to the attention of the various parties involved in the reintegration of sick employees and is among the most viewed publications on the website.

- **Police files**
  The investigation into the files of the Criminal Investigation units of eight regional police forces that was started in 2003 was finalised in 2004. The general findings of the investigation have been published.

- **Investigation into wire tapping rooms**
  At the end of 2004 – later than anticipated – the Dutch DPA started the preparations for an investigation into the privacy aspects of data processing in police wiretapping rooms, in a follow-up to the 2003 Investigation into the safeguarding of confidential communications of solicitors in the interception of telecommunications. The investigation will not be completed until 2005.

- **Camera surveillance**
  Building on the investigation *Camera surveillance in public spaces - an investigation into the deployment of camera surveillance in all Dutch municipalities* (2003) a study was published in December 2004 on the privacy aspects of camera surveillance in public areas. *Cameras in the public domain - privacy standards for camera monitoring of the public order* offers municipalities rules of thumb for decision-making and implementation of camera surveillance. The study is one of the most viewed publications on the website.

- **Citizens Service Number**
  The realisation of the Nationale Vertrouwensfunctie, an organisation that will be charged with providing citizens with insight into all the information flows based on the citizens service number, experienced a delay in 2004. Unfortunately in 2004 it was not yet made possible for the Dutch DPA to start verifying existing and new data processing procedures and preparing for the future Ombudsman function. This preparation will now be realised in 2005.

- **Certification**
  The system of privacy certification devised in collaboration with NOREA (professional association of IT auditors) and NIVRA (Royal Dutch Institute of Registered Accountants) was tested in practice in 2004 using experimental certifications. Deviating from what was intended initially, and in close consultation with the partners, the choice was eventually made to leave the ultimate construction of certification systems entirely to the market parties. The project was completed in February 2005 with a presentation and publication of the document entitled *Contours for Compliance - a guide for the definition of standards within the Privacy Audit Framework* to interested organisations.

- **Introduction of DBC system**
  In the area of health care the Dutch DPA will remain closely involved in the development and implementation of the financing system based on the Diagnosis Treatment Combination.

- **National registers in the care sector**
  In 2003 the Dutch DPA completed a preliminary investigation into five national registers in the care sector. Later than anticipated, general findings and standards for national care registers were formulated in 2004 on the basis of the study.

- **Investigation into the way privacy is experienced**
  In 2004 the Dutch DPA instructed TNS Nipo consult (a market research agency) to carry out a study into the way Dutch citizens experience privacy and what their privacy requirements are. Similar studies have already been carried out in a number of European countries. The results will be published in 2005.

- **Policy rules and 2nd line position**
  The Dutch DPA has published a number of policy rules for the treatment of certain categories of cases and the associated publicity. In the context of the endeavour toward a 2nd line position the Dutch DPA was able to reach agreements with a number of sector, trade, umbrella and professional organisations regarding information exchange and distribution of tasks in the provision of information and processing of complaints.

- **Organisational development**
  In 2004 the Investigations department became operational. A start was made on the development of differentiated research formats and risk analysis as a tool for policy formulation. The department played an important role in the Nipo study into the way citizens experience privacy and also performed the 2004 notifications analysis.

- **Dutch DPA website**
  At the end of October 2004 the Dutch DPA went live with a new website aimed at providing more direct information to data subjects and data controllers. The material on the website has been made accessible in a more demand-focused way. Since the website has been upgraded the number of visitors has increased notably.

of privacy must be sufficiently justified. Neither were the possible discriminatory and stigmatising effects of the proposal acknowledged. On 1 January the extended and de facto general duty of identification came into force.

Cameras in the public domain

The interest in video surveillance has only increased in recent years. The general public also accepts cameras, expecting video surveillance to be effective. Video surveillance, particularly on the part of the Government, has increased considerably in recent years. This is why, in 2003, the Dutch DPA initiated a study into the nature and scope of video surveillance by Dutch municipalities. Among other things this study showed that 20 percent of municipalities use video cameras and that in many of these municipalities the effectiveness of the video surveillance had not (yet) been evaluated. Subsequently, a study entitled Cameras in the public domain was published in November 2004 with rules of thumb for decision-making, starting points for the placement and use of cameras, the rights of data subjects, monitoring and evaluation.

Administrative records

The new WAO (Occupational Disability Insurance Act) and the insurance companies
In respect of the new WAO system the Dutch DPA advocated greater clarity about the positions the various parties (employer, employee, UWV [employed persons' insurance administration agency], reintegration agencies and insurance companies) take up in relation to each other when it comes to the use of personal data. The way in which insurance companies will deal with personal data in the new system is unclear, and this is not a desirable situation.

As a result of the new tasks pursuant to the Work and Income based on Employment Capacity Act but also, for instance, the new Health Insurance Act, the corporate groups of which the insurance companies are a part will have access to even more (medical) personal data. This creates the potential for a powerful and influential information position.

Insurance companies do, however, acknowledge the importance of the careful processing of personal data. If the Government fails to establish rules for this type of processing it will be time-consuming and inefficient for the parties involved in the processing. The Dutch DPA has therefore urgently advocated to the Minister of Social Affairs and Employment that clarity must be provided in the relevant legislation regarding the possibilities and limitations relating to the processing of personal data.

Diagnosis Treatment Combinations

Further to the formulation of the privacy framework by the Ministry of Health, Welfare and Sport (VWS) and Zorgverzekeraars Nederland (Association of Dutch Health Insurers), it was agreed with the Dutch DPA that the privacy-conscious introduction of the Diagnosis Treatment Combinations (DBCs) would be given a follow-up. The sharing of information between the different parties must be done in such a way that there is less detriment to the patient's privacy and to medical confidentiality. The Dutch DPA played an advisory role for a number of work groups. The Dutch DPA also took a critical look at the structure of the DBC Information System. Agreements were reached with the Ministry of Health, Welfare and Sport and other parties involved regarding minimum guarantees for the coming period. These periodic meetings between the Dutch DPA and

the different parties will continue in 2005. As the supervisory authority, the Dutch DPA will remain very alert to the parties' honouring of their promises.

New police information system

In recent years the different police forces have developed a colourful range of ICT applications to perform the same tasks. Eventually the decision was made to try to achieve countrywide uniformity in the area of ICT. As the supervisory authority for the processing of data by the police, the Dutch DPA was asked to advise regarding the statutory rules that affect the choice of new systems.

In addition, work also commenced on the revision of the statutory framework for a police information system. In 2004 the Minister of Justice received advice regarding the draft legislative proposal on the Police Data Act. The Dutch DPA is able to agree with a system for processing police data in which the guarantees increase as the processing constitutes a greater risk for the data subjects involved. There were also three important areas of criticism. Firstly, more emphasis is needed on the quality of data processed by the police. Secondly, the Dutch DPA seriously objects to the introduction of so-called theme files: large collections of data about citizens who are not suspected of anything. Thirdly, clear regulations are required in respect of retention periods. Data that is no longer required should be destroyed rather than retained indefinitely 'just in case' the information might be needed in future.

New Schengen Information system

The purpose of the Schengen Information system is to reinforce control on the outer borders of the European Union. The simple fact that new member states have joined the EU makes it necessary to update this system. Neither can biometric characteristics be included in the system. In September 2004 the Joint Supervisory Authority (JSA) Schengen, under the presidency of the Dutch DPA, issued an opinion about the development of the new Schengen Information System (SIS II). The JSA requests attention for the protection of personal data even in the design stage of SIS II. The European Council is called upon to clarify the objective and functions of the new system so that sufficient privacy guarantees can be incorporated.

European visa information system

Plans exist for one visa information system for the entire European Union, using biometric data. The Article 29 Working Party published an opinion on these plans in August 2004. The Work Group points out that the processing of biometric data must meet stringent lawfulness standards because the risk of abuse of such data is great. The Working Party has serious reservations about the routine, large-scale storage of biometric data and wants to be involved in the further structuring of the visa information system.

Citizens Service Number

The policy for an 'electronic Government', a government that makes optimum use of information technology, including the Internet, was outlined in 2004 in the programme entitled 'A different Government'. The introduction of the Citizens Service Number (BSN) is an absolute condition for the success of this programme. The BSN program agency was established with the instruction to implement the plan that was finalised at the end of 2003.

The Government unexpectedly made the decision – contrary to its earlier promises – to introduce the BSN in the health care sector as well. Health care institutions and health insurance companies will be obliged to use this number. The use of a unique personal identification number in the health care sector has inherent risks. Large-scale linking of (patient) data becomes easier and, therefore, so does abuse. However, a separate care identification number – a safeguard against the too-easy distribution of information on patients and health care recipients – no longer proved feasible in the political and social arena. The Dutch DPA subsequently approved the use of the BSN in the health care sector, provided it was accompanied with compensatory guarantees, including reliable authorisation procedures for the use of medical data that becomes accessible with the number.

In 2005 the Dutch DPA will play a part in the preparation of the so-called Nationale Vertrouwensfunctie, an organisation that provides for structural monitoring in the form of, among other methods, one office where citizens can take their questions and complaints about the BSN.

Codes of conduct

In 2004 it was possible to approve five sectoral codes of conduct. After a preparatory process spanning many years, in which the Dutch DPA tried to support the sector association, the code of conduct for private investigation agencies was approved early in 2004.

The Royal Professional Association of Court Bailiffs developed a code of conduct comprising rules for the special situation whereby court bailiffs act as public functionaries and also provide commercial services (for instance debt collection). It is essential that they do not use the information obtained pursuant to their special legal status as a civil servant in the performance of their non-public activities.

The sector organisation for Recruitment, Search and Selection (OAWS) revised and updated its code of conduct that indicates for which purposes personal data of potential candidates can be processed. The 'Good Behaviour Code of Conduct', a code of conduct for health research, was also revised and rules for the processing of patient data in health research have been incorporated. New is the code of conduct for the processing of personal data in research and statistics, which was formulated by three organisations: the Association for Policy Research, the Association for Statistics and Research and a professional association for market and policy researchers (MarktOnderzoekAssociatie.nl).

In 2004 Zorgverzekeraars Nederland, the sector association for health insurance companies, started on the formulation of rules of conduct for, among other things, the use of the large quantities of medical data that health insurance companies receive in the context of healthcare claims. Rules will also be formulated for the investigation of fraud committed by an institution, care provider or insurant. This concerns an addition to the Code of Conduct for the Processing of Personal Data of the financial institutions. Expectations are that these rules of conduct can be furnished with an approval in the summer of 2005.

Supervision

The annual Spring Conference of the Data Protection Authorities in the European Union, which in 2004 was organised in Rotterdam by the Dutch DPA, focused on effective supervision methods and arrangements. The three-day conference was opened on 22 April by Minister of Justice J.P.H. Donner, who called for further collaboration in supervising the enforcement of law and order in Europe within the so-called third pillar, the policy area of the Ministries of Justice and Internal Affairs. The European privacy regulators have now intensified their collaboration in monitoring and advising on the areas of responsibility of the police and the Ministry of Justice.

Supervision of the European collaboration in law enforcement

The national Data Protection Authorities in the European Union jointly supervise the institutions in which the national police and Ministry of Justice authorities in Europe collaborate (among others Europol and Schengen), via the so-called Joint Supervisory Authorities and Bodies. In 2004 these supervisors of personal data processing (Schengen, Europol, Customs and Eurojust) met for the first time with a view to providing stronger advice regarding the third pillar. Among other things, they issued a response to the questions of a Commission of the British House of Lords regarding the combating of terrorism in the European Union and privacy protection.

The regulators advocated improvements to the protection of the fundamental rights of the individual in respect of his personal data and the supervision thereof. Existing international legislation and regulations are not sufficient for this purpose. In view of the increasing scale of data processing, often including data on persons who are not suspects, there is a need for new specific rules for the police sector.

Private investigation

In 2004 a special supervisory arrangement was created for the private investigation sector. The Act for Private Security Organisations and Detective Agencies does standardise the sector, but rules for the realisation of investigations and the further processing of the data collected in such investigations were lacking. The scope of the code of conduct of the Association of Private Security Organisations, which provides for this, was expanded because the Minister of Justice made this code of conduct mandatory for all private investigation agencies by Ministerial decree. The Dutch DPA and the Minister of Justice have entered into collaboration for the monitoring of compliance with this code of conduct.

Work and Assistance Act

For the purpose of monitoring compliance with the new Work and Assistance Act the IWI (Work and Income Inspectorate) and Dutch DPA have expressed their intention to enter into a collaboration agreement in 2005. Through collaboration and the sharing of knowledge more effective and efficient supervision will be possible. Collaboration also promotes unambiguous supervision because the standards used by the regulators can be coordinated. This can also lessen the regulatory pressure for organisations under supervision. For example, the agreement will stipulate arrangements in respect of sharing supervisory information and the mutual provision of information regarding the results of investigations.

Objectives in 2005

IN 2005 THE FOLLOWING ISSUES AND OBJECTIVES WILL BE PRIORITISED:

- **Security and privacy**
  Security and privacy are not necessarily mutually exclusive. The Government's endeavour to achieve a much stronger information position with regard to citizens (who are mostly not suspected of anything) does however raise some essential questions. The supervision of the way certain powers are used and of the information gathered on citizens is, wrongly, not yet sufficiently regulated. Where supervision and control are regulated, there is sometimes poor compliance with the rules. In a response to the developments in the area of security and the combating of terrorism the Dutch DPA will, in 2005, publish its standpoints and consider the investigations that need to be carried out into compliance with privacy rules in this area.

- **Special police registers**
  The Dutch DPA considers it one of its tasks to provide structural supervision of the special police registers, as these are not or hardly accessible to citizens or to the courts. In 2005 the Dutch DPA will once again investigate a number of files from these registers and publish a report of its general findings.

- **Private investigation agencies**
  In 2005 the Dutch DPA will investigate compliance with the sectoral code of conduct by private investigation agencies, by means of a random check.

- **Risk selection**
  Profiling is the assessment of individuals on the basis of group characteristics. This concerns inclusion and exclusion of people on the basis of an analysis using a profile. Profiling has the inherent risk of unfair treatment. This year the Dutch DPA will organise an expert meeting on risk selection. Based on the results of this meeting the Dutch DPA will decide whether it will further define, in a publication, the privacy rules for the use of group profiles in risk selection.

- **Internet and privacy**
  The Internet confronts users with questions about their privacy, the security of their personal details and the possible abuse of these details. The Internet also confronts the Dutch DPA with new questions about its authority as a regulator and the effective supervision of the Internet. The Dutch DPA will determine and publish its position as a regulator in respect of the Internet. This also includes the formulation of specific standards in a number of areas. The focus will be on publications on websites, seen from the angle of the privacy problems that citizens experience on the Internet in everyday practice.

- **Information obligation**
  Authorities, companies and other organisations have the statutory obligation to inform people whose personal data they use of this fact and its purposes. Compliance with this information obligation is an important guarantee that citizens are able to exercise their rights in respect of their personal data. The information obligation is being insufficiently complied with. The Dutch DPA will pay extra attention to this in 2004, both in its information provision and by means of investigations. Compliance with the information obligation will be investigated, particularly also among private detective agencies and in respect of combating Social Security fraud.

- **Investigation of the notification obligation**
  Also in 2005 the Dutch DPA will carry out a random check of compliance with the notification obligation in a number of sectors, based on an analysis of the public register of notifications.

- **Administrative burden**
  The Dutch DPA will formulate proposals for the reduction of the administrative burden experienced by companies (and authorities), whilst retaining the current level of protection of personal data. Further to proposals made toward the end of 2004, the Dutch DPA will enter into consultations with the Minister of Justice to discuss a broadening of the exemptions of the notification obligation. The Dutch DPA will also suggest that the permit obligation for the transfer of personal data outside the EU be abolished if companies use standard contracts approved by the European Commission.

- **Binding Corporate Rules**
  The Dutch DPA will actively contribute to simplifying the rules for the transfer of personal data to data controllers outside the European Union. Among others the Dutch DPA will work toward European agreements in respect of a uniform procedure for applying for permits and in respect of co-ordinated processing of permit applications based on so-called binding corporate rules (BCRs): self-regulation tools for the processing of personal data within companies operating on an international basis.

- **Collaborations**
  Collaborations aimed at dealing with social issues (safety, nuisance in neighbourhoods, outreach assistance, youth care) are receiving a lot of attention. In this context privacy legislation is often – and often wrongly – seen as an obstruction. The Dutch DPA will contribute to clarifying the rules for the necessary exchange of personal data in collaborations. In April 2005 the Dutch DPA is organising a symposium on privacy in collaborations. Together with Vide, the professional association for regulators, the Dutch DPA will organise a symposium for inspectorates etc. about their position as a participant in collaborations and as a regulator of organisations that participate in collaborations.

- **Supervision and regulators**
  The Dutch DPA aims for efficient and effective supervision of compliance with the rules for processing of personal data. Umbrella and trade organisations will be contacted regarding their responsibility for self-regulation, among other means by the publication of a guide for compliance assessment. The Dutch DPA also stimulates the appointment of data protection functionaries and, in 2005, will focus on the qualitative improvement of this internal supervision.
  The Dutch DPA will issue advice to the Minister of Justice aimed at resolving obstacles the regulators are faced with as a result of the Personal Data Protection Act.
  The Dutch DPA will enter into a collaboration with the OPTA. With a view to effective supervision, collaborations with various other regulators (including the IWI) will also be assessed. Together with the Equal Treatment Commission, the National Ombudsman and the Study and Information Centre for Human Rights, the Dutch DPA aims to advise the Government on the desirability of a National Human Rights Institute.

- **Health Care and Social Security**
  The introduction of market mechanisms and increased individual responsibility are focal points in both sectors. In both systems insurance companies are given a prominent role that will result in a more intensive collection of often sensitive data on individual citizens and the exchange of this information within conglomerates. However, clear rules for the use of personal data are lacking.
  The Dutch DPA will continue to highlight the privacy risks associated with the partial privatisation of health care and security systems. As a regulator the Dutch DPA will closely monitor the introduction of the Diagnosis Treatment Combinations (DBC) system. An exploratory investigation among health insurance companies into the use of medical data by health insurers will also be carried out.
  In 2005 the Association of Dutch Health Insurers (ZN) will revise the addendum to the Code of Conduct for financial institutions and expand its scope with rules for material controls and rules about the use of claim details. The Association will submit this addendum to the Dutch DPA for approval.
  A normative framework for the social services will also be published: ten basic principles the social services must comply with when processing personal data.

- **Citizens Service Number**
  The introduction of the citizens service number (BSN) is currently the focal point in the development of the Government information infrastructure. The Dutch DPA was intensely involved in the preparation of this system. Through participation in the BSN steering committee and in the working party for the Nationale vertrouwensfunctie (an organisation that will be charged with providing citizens with insight into all the information flows based on the citizens service number), the Dutch DPA aims to ensure that the agreed privacy guarantees are in fact realised. In the context of the *Nationale vertrouwensfunctie* the Dutch DPA itself will be responsible for the National Ombudsman function and the verification of data exchange based on the BSN and will be preparing for the implementation of these tasks in 2005.

- **Evaluation of the Personal Data Protection Act**
  The Dutch DPA will prepare to make a contribution to the evaluation of the Personal Data Protection Act, which is expected to take place in 2006 (Article 80 of the Personal Data Protection Act).

Health Insurance Act

The new Health Insurance Act provides for a mandatory standard of health insurance for all residents. In 2004 the Dutch DPA advised that, in respect of the legislative proposal, more concrete standards be set for the use and exchange of personal data in the context of health insurance. The structural supervision of health insurance companies would otherwise mainly be limited to highlighting unlawful situations in insurance-related, financial and administrative areas. Supervision of the processing of personal data must also be specifically included in the legislative proposal because the processing of personal data by the health insurance companies also requires structural supervision. In addition the draft addendum of the Association of Dutch Health Insurers (ZN) with the Code of Conduct for the Processing of Personal Data for financial institutions must be adjusted.

Spam

Unsolicited e-mails sent in large quantities, better known as spam, are a nuisance, are difficult to eliminate and incur high costs for Internet service providers, and therefore for their customers. According to recent estimates approximately three quarters of all e-mails sent worldwide are spam. The European Directive on Electronic Communications (2002/58) prohibits the sending of unsolicited commercial messages and the European regulators supervising compliance with this prohibition work together in the so-called Contact Network of Spam Authorities to exchange information and facilitate collaboration in the enforcement of the prohibition in the EU. A collaboration agreement has also been formulated for this purpose.

In the Netherlands the OPTA (Independent Post and Telecommunications Authority) and the Dutch DPA signed, on 19 October 2004, agreements regarding collaboration in respect of the prohibition on spam, which in the Netherlands has been in force since 19 May 2004. The Dutch DPA will focus primarily on supervising the collection and use of e-mail addresses. Individual complaints regarding spam can be addressed to the OPTA via www.spamklacht.nl. The practical agreements about dealing with spam constitute a prelude toward a broader collaboration protocol in 2005.

Investigation and enforcement

Criminal investigation units

In 2003 and 2004 the Dutch DPA carried out investigations into special police registers held by the criminal investigation units (CIE) of the regional police forces. Pursuant to the Police Files Act (Wpolr) the Dutch DPA is the regulator supervising the use of the police files. In this position the Dutch DPA has access to the content of the CIE files. Because of their sensitive nature these files are, quite rightly, largely protected from access by the registered persons involved and from supervision by the court. In this context the Dutch DPA considers it a special responsibility to substantively supervise the CIE files.

In its investigations the Dutch DPA focused mainly on checks based on the content of the files, and a number of technical and organisational aspects were also taken into consideration. The general picture emerging from the investigation is mostly positive. The substantive aspects that were investigated generally proved to be in order. With regard

to the investigated technical and organisational aspects it became clear that on a number of points the rules imposed by legislation and regulations are not being met. The police forces have indicated that, whilst awaiting an information system to be implemented on a national basis, they will not make any adjustments to the current systems and methods.

Schengen Information system

In 2004 the JSA Schengen asked the national supervisory authorities of the member states linked to the Schengen Information System (SIS) for an investigation into the practice of registering foreign nationals in the system. JSA Schengen received reports at the end of June 2004 and the end of December 2004. A number of registrations have raised questions for the Dutch DPA and these registrations will be investigated further.

National registers in the health care sector

In 2004 the Dutch DPA completed its investigation into the operation of national registers in the health care sector with a report that was published in April 2005. The key questions of the exploratory investigation were: what does the patient know about the registration of his data in national data banks, for what exact purposes are these registers used and can the information in these registers be traced back to the individual patients. In view of the sensitivity of the information and the professional secrecy that applies to physicians, partly in view of this sensitivity, the law currently only offers limited possibilities for the processing of (indirectly) traceable patient data.

The investigation of five national registers gave the Dutch DPA the impression that the investigated national registers generally handle the personal data reasonably well. It also emerged that, in nearly all cases, improvements were possible and necessary. The main measure to be implemented is limiting the traceability of the data to individual patients. A number of recommendations have now been adopted by the registers.

Compliance with the notification obligation

Pursuant to the Personal Data Protection Act (WBP) companies, organisations and institutions are obliged to notify the processing of personal data to the Dutch DPA or their Data Protection Officer, unless there is an exemption. If data processing has wrongly been notified incorrectly or incompletely, or has not been notified at all, the Dutch DPA can impose a penalty to a maximum of 4,500 Euro. Notifications from certain sectors or regarding certain types of processing are periodically subjected to a further investigation. The Dutch DPA also carries out such investigations as a result of complaints from data subjects.

In 2004 the annual investigation focused on three sectors, namely telecommunications, mental health care and the debt collection sector. The investigations will be finalised in 2005 and sanctions may or may not be imposed.

As a follow-up to specific information provided to the telecom sector the Dutch DPA checked whether a number of providers of telecommunications services (fixed and mobile telephony and Internet) complied with the notification obligation. This investigation focused specifically on the notification of the processing of telecommunication traffic data.

In a number of Area Health Authorities (GGDs) the Dutch DPA investigated the notification of the processing of personal data in the context of the Public Mental Health

Care (OGGZ). It is the legislator's opinion that this processing carries specific risks for the privacy of the citizens involved; when notifying the Dutch DPA of the processing the data controller must therefore also request an investigation into the lawfulness of the processing, the so-called preliminary investigation.

Analysis of the WBP notifications register showed that the number of notifications by debt collection agencies lags behind considerably. Supervision in this sector was aimed at investigating to what extent debt collection agencies process personal data and to what extent they rightly failed to notify the processing of personal data.

Penalties for municipalities and companies

In 2003 the Dutch DPA performed the first random check on the compliance with the WBP notification obligation among a number of municipalities, health insurance companies, internal and external Occupational Health & Safety services (arbodiensten) and direct marketing companies. The number of WBP notifications increased strongly after these initial checks, not only in the investigated sectors but also among the private detective agencies, the police and in the health care sector.

A total of 50 investigations were carried out in the context of this initial check. In a number of cases a supplementary check was carried out on site in order to establish the facts. At the end of 2003 the random check resulted in the first penalties for a municipality and two companies.

In the course of 2004 the CPB imposed a total of 29 penalties ranging from € 3,000 to € 15,000. In a number of cases the Dutch DPA used its authority to reduce the penalty, especially if, as in the case of municipalities, there was a high level of processing of personal data. The main consideration was that even a reduced penalty would achieve its objective, namely a special and general preventative effect.

The aforementioned penalties were imposed on 14 municipalities, 3 direct marketing companies, 3 health insurance companies and 9 Occupational Health & Safety services. Most municipalities submitted an objection against the penalty; a number of municipalities have now paid the penalty. None of the private organisations except one submitted an objection and nearly all have now paid. All the organisations involved have now notified the Dutch DPA of their processing of personal data.