

2006 in a nutshell

The protection of privacy inspires a wide range of reactions. A very common one is 'I don't really think it's necessary. I've nothing to fear, because I've nothing to hide and security is more important than my privacy.' Or, for example 'It doesn't make any difference to me. They already know everything about you.' Or 'It's a really important thing, because you don't want to live your life being permanently spied on.'

The Dutch Data Protection Authority (Dutch DPA) continues in its efforts to strike a proper balance between the interests of security, control and utility, and to guarantee as far as possible the protection of the private life of individuals, which can come under pressure from those interests.

The right to integrity of one's private life, inseparably linked with careful use of personal data, is less and less something to be taken for granted. The Dutch DPA has a duty to act as a 'privacy watchdog' where there is any threat that this basic right might be overlooked in the interests of security and criminal investigations, or that it might evaporate in the limitless scope of the Internet and other technological developments. Its primary function is to keep a check on compliance with the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act]. But effective supervision and, where necessary, enforcement of the rules for dealing with personal data is not enough. By providing information and advice, and by consulting with social parties, the Dutch DPA adopts a proactive stance in order to persuade citizens, governments, companies and institutions of the necessity of handling personal data with care. This is in order to enhance the confidence that ordinary people, who have nothing to hide, should be able to have in institutions dealing with their data. It is also designed to improve the quality of legislation and service provision.

This chapter provides an overall summary of the work of the Dutch DPA during the past year.

Security and control

The protection of the private life of individuals is beset on two sides. On the one hand, for reasons of political security, governments are proactively and dramatically extending their powers at national, regional and international levels to collate large quantities of data concerning ever larger groups of citizens.

On the other hand, continually refined technology and the interlinking of data files provide ever more opportunities for tracking and recording the comings and goings of everyone.

The international conference of the data protection authorities, attended annually by the Dutch DPA, issued a warning in November 2006 that, as regards the protection of data, the question was whether the traditional supervisory methods were still adequate, in light of the new technologies. The supervisory agencies consider that joint action to counteract excessive forms of control is now necessary.

Passenger information

A new agreement will come into effect in August 2007 at the latest between the United States and the European Union concerning airlines providing passenger information to the USA. The 'Article 29 Working Party' of European data protection authorities, of which the Dutch DPA is a member, is concerned about the current temporary arrangements that form the basis for the proposed treaty, because they appear to facilitate an even wider dissemination of information among American authorities, for even more new purposes. The Chairman of the Dutch DPA emphasised during a meeting in December 2006 in Brussels that it had to be made clear that the security measures to be taken are necessary and proportionate, and also pointed out the importance of transparency and accountability.

Cooperation in the EU by Justice and the police

The decisiveness of EU member state governments in relation to the introduction of security measures based around cross-border exchange of information stands in stark contrast to the adoption of the European Framework Decision on personal data protection for collaboration between Justice and police. According to the European data protection authorities, the only



workable option for a more extensive exchange of personal data is a harmonised high standard of protection in the third pillar. The same applies in relation to transfer of information to countries outside the EU and to international institutions. The European data protection authorities consider that a limited approach will not be workable in practical terms, and will also have an adverse impact on confidence in the collaboration between police and Justice at European level.

Detection of terrorist offences

In the Dutch context of counterterrorism in recent years, there has been an accumulation of powers in the hands of the police and judicial authorities. The Dutch DPA has provided advice to the Minister of Justice and the Lower House of the Dutch parliament in recent years on legislative proposals to extend the scope of the detection and prosecution of terrorist offences. The Dutch DPA's criticisms are aimed primarily at the absence of clear justification of the need for the proposed measures, including more broadly targeted preliminary research into particular groups within society. Because many of these points of criticism were not followed up, the Dutch DPA provided more detailed advice last year to the Senate Standing Committee on Justice, at the request of the chairman of the Senate, regarding the measures he considered were necessary in order to achieve a better balance between supervision of the processing of personal data and the growing powers of the penal authorities.

Topic processing

The shifting boundary between investigative and prosecution powers has clear implications for the protection of personal data. One of the major innovations in the new *Wet politiegegevens* [Police Data Act] is introduction of "topic processing". Topic processing includes the systematic and proactive processing of personal data in relation to 'innocent' citizens - people against whom the facts and circumstances do not raise any reasonable suspicion of guilt. By contrast with the current *Wet politieregisters* [Police Registers Act], the new act will not have any separate regime for data relating to these 'slightly suspect' individuals. The Dutch DPA would warn that without extra protection for this personal data, for example by means of coding, there will be an unacceptably high risk of citizens being wrongly subjected to police action. In 2006, the Dutch DPA discussed with the Senate Standing Committee on Justice the need for permanent monitoring of the accuracy and quality of police data.

The virtual moat

In 2005, the Raad van Hoofdcommissarissen [Association of Chief Police Officers] put forward the notion that the police would start to focus on the infrastructure carrying people, money, goods and information, in the context of their offensive against crime. One of the ways this would happen would involve detection using cameras aimed at access routes into cities. The Dutch DPA expressed its concerns about this proposal to the Minister of Internal Affairs and Kingdom Relations, distinguishing between three degrees of acceptability in the proposed method of operation. Identifying suspects using registration plate recognition, and recording their details, would be acceptable. Recording details of repeat offenders - those known to the police - without them being suspected of a crime at that point would not be acceptable as a matter of course. There would have to be a check, on a case-by-case basis, as to whether the storage of this data was in breach of the law. Recording the details of everyone travelling on a particular route would be taking things too far, according to the Dutch DPA, certainly if these details were subsequently analysed.

These types of new methods, under which protection of personal data would be likely to suffer, should only, in the view of the Dutch DPA, be considered if the police can show that their existing powers are inadequate for guaranteeing further security. The Dutch DPA held

consultations with the Raad van Hoofdd commissarissen in the first quarter of 2007 concerning their experience with the system to date.

Large-scale data processing

Technical developments have now made it possible for governments, other service providers and trade sectors to process data, including personal data, on a large scale. This can be both useful and lucrative, but it can also be damaging to individuals if things go wrong. What needs to be done is to try and avoid such errors at the design stage, both as regards the technology and the legislation.

Passports

Passports are provided with biometric information in the member states of the European Union. In this context, the Netherlands will shortly have a central storage point for travel documents, which will also include biometric data for the applicants. Why is there a need for this type of central storage? Are the government's arguments for this convincing? These and other questions concerning usage, need and the potential disadvantages of this large-scale storage of data were discussed during an expert meeting organised by the Dutch DPA in February 2006. The results of the discussion were ambiguous: central collation of biometric data can on the one hand protect identities by having one central reference point, but on the other hand they can undermine that protection as a result of security risks and potential use of biometric data for other purposes.

The Citizens Service Number

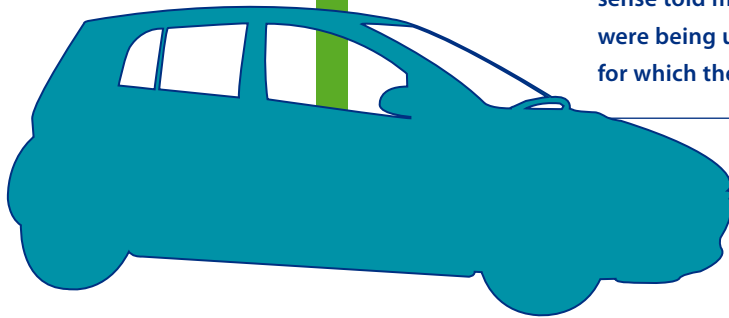
The introduction of the burgerservicenummer (BSN) [Citizens Service Number] is once again a topic for discussion in the Dutch DPA annual report. Since 2004, when the first opinion on the Bill was presented, the Dutch DPA has been busy convincing the Minister and Parliament of the need to build in safeguards in some essential elements of the Act for a careful processing of citizens' personal data. After all, if something goes wrong with the information chain in back offices through the use of the BSN and its associated personal data, the oil slick effect of the dissemination of such information will often mean that the consequences for a citizen will be incalculable. The Act offers inadequate facilities for restitution in the circumstances. This is unlikely to promote the confidence that citizens should be able to have in the way in which the government deals with their personal data.

The introduction of the BSN, planned for 2006, has been postponed. The intention is that, from 2008 onwards, it will replace the present social insurance number in the healthcare sector. This 'BSN-z' will be used for patient-related communication between care providers, healthcare insurers and diagnostic bodies. It will be essential here to ensure that the recording of personal data is done with extreme care. Many general practitioners had already started to record their patients' social insurance numbers in preparation for the 'BSN-z'. Because of the errors in the numbers that the patients had provided, the Landelijke Huisartsen Vereniging [National General Practitioners' Association], at the request of the Dutch DPA, scrapped all references in its information material to the topic of asking for social insurance numbers.

The other pillar of the BSN system in health care is mandatory identification. The Dutch DPA, generally not a supporter of obligatory identification, nonetheless feels that it is very important in health care, bearing in mind the health risks that incorrect identification might involve for patients. General practitioners find it irksome to have to ask their patients for proof of identity.

> **Cameras used for survey**

As he read a teletext report, a motorist wondered whether the Ministry of Public Works and Water Management was not going too far in recording details of road users on the A2. He read that cameras were being used to ask road users to cooperate in a survey regarding road works on this highway. "My common sense told me something was not right. These cameras were being used for something other than the purpose for which they had been put there."



The Lower House appreciates this and has adopted a motion that will relax the obligation of identification into a duty of verification in the Decree on the use of the BSN. The Dutch DPA advised the Minister not to follow this through, or at least to adopt additional measures in order to ensure that, once a patient's identification has been confirmed, this data would be available for audit in such a way that cases of mistaken identity are excluded.

The BSN will be used to facilitate the creation of the Elektronisch Patiëntendossier (EPD) [Electronic Patient File]. The Dutch DPA is actively involved in its development. The primary concerns here should be the proper regulation of accountability, access, security and supervision in relation to the file.

The public transport chip card

At the start of 2006, the Dutch DPA published the conceptual document Privacy en de OV-chipkaart [Privacy and the public transport chip card]. The Dutch DPA's objections against transport companies using travel data from named cards for service provision and direct marketing purposes resulted in the Lower House pressing the Minister to resolve the privacy problems. To deal with this issue, the Minister attempted, in consultation with the NS [the Dutch national railway system] and the Dutch DPA, to define and resolve a number of bottlenecks. During 2007, the Dutch DPA will carry out research with one of the public transport companies that has partially introduced the OV-chipkaart, to see whether and how the measures for protection of personal data are being implemented.

The digital customer file

More efficient commerce, more effective anti-fraud activities and an improvement of the provision of services to the citizen are the aims of the digital customer file as proposed in the Wet eenmalige gegevensuitvraag werk en inkomen [Act for a single data questionnaire for employment and income]. The Bill provides for a single collection of all data pertaining to a client, drawn from organisations such as social services, the CWI [Employment and Income Centre], the UWV [Employee Insurance Implementation Body], the Sociale Verzekeringsbank [National Insurance Bank], de Rijksdienst voor het Wegverkeer [National Road Transport Department] and the Informatie Beheer Groep [Information Management Group]. The digital customer file that will be prepared from this data is intended to avoid the government having to

Results for 2006

The previous annual report included an overview of the targets for 2006. Put briefly, this is how things now stand:

> European investigation into health care insurers

The European data protection authorities have carried out coordinated research into the processing of personal data by the private health care insurance sector. The results of the investigation will be published in 2007.

> Security of information at hospitals

The Dutch DPA and the Inspectie voor de Gezondheidszorg [Dutch Inspectorate for Healthcare] signed a collaborative protocol in November 2006. The purpose was to achieve effective supervision of the use of personal data in the healthcare sector including electronic patient files. Pilot studies were carried out during 2006 for a wider-ranging joint investigation in 2007 into security of information at hospitals.

> Electronic child file

The intention behind the electronic child file (the EKD) is to record a child's development from birth (or earlier) and also the child's environmental indicators. Bringing the EKD online for youth health care was postponed until 1 January 2008, and it is not expected to become compulsory by law until 2009. During 2006, the Dutch DPA again pressed for answers to the most important privacy issues involved in the EKD. It will continue its intensive tracking of developments in 2007, particularly where there is any consideration being given to possible use of the data outside the health care sector, for example in any national reference index of young people at risk that might be introduced.

> Intervention teams to combat fraud

Various government organisations collaborate within intervention teams on combating fraud in relation to social security. It can prove necessary in such situations, based on in-house observations, to collect and establish data in relation to individuals without them being aware that this is happening. The Wbp obliges organisations to inform the parties concerned about these 'secret observations', even if they do not discover any damaging material. The way that the intervention teams deal with secret observation is established in the procedural description *Heimelijke waarneming door de interventieteams* [Secret observation by intervention teams]. A revised version of this procedural description was approved by the Dutch DPA in 2006. An investigation into working methods, prepared in 2006, was recently commenced for a number of intervention teams.

> Combating fraud in social security

In order to stop abuse of public funds as far as possible, local authorities are keen to, as far as they can, verify information taken from benefit applicants against other sources of data at an early stage of their contact with the applicant. Local authorities also want to unlock and link up an increasing number of data files in their efforts to combat benefit fraud. In 2006, the Dutch DPA issued the notice entitled *Fraudebestrijding door bestandskoppeling* [Combating fraud by linking files]. This indicated the points requiring attention in order to strike a balance between combating fraud and respect for the private life of individuals.

> Binding Corporate Rules

Binding Corporate Rules are internal codes of conduct produced by multinationals, under which they can obtain a permit for passing on personal data to their associated group companies based in other countries. The first coordinated European permit procedures commenced in 2006, and the first BCR's were approved via these procedures in several countries.

> The duty to provide citizens with information

Transparency concerning the processing of personal data is one of the pillars of the Wbp. An investigation was carried out by the research bureau TNS NIPO on the instructions of the Dutch DPA at the end of 2005 in three sectors, namely general practitioners, educational institutions and housing associations, focusing on compliance with the duty to provide information under the Wbp. Research was also carried out into compliance with the duty to provide information as experienced by citizens. The research findings were published in May 2006. The recommendations from the research will result in better awareness of and better compliance with the duty to provide information.

> Internet publications and privacy

Internet users are faced with questions regarding their privacy and the use of their personal data. The Dutch DPA is continuing to work on establishing the facilities for effective supervision on the Internet. An initial version of a discussion document on this subject was debated during an internal symposium. It is expected that guidelines will be published in 2007.

> **RFID**

An external discussion document from the Dutch DPA concerning the social implications of the use of Radio Frequency Identification was published in October 2006. RFID is a technology which allows all sorts of items of property, as well as people and animals, to be equipped with information chips that can be read even at a distance. The sorts of information that can be stored on the chip, and what subsequently happens with that information, are increasingly impacting on the sphere of personal data protection. The report is now also available in an English-language version, and forms the basis for further brainstorming and consultation on this subject.

> **Biometrics in travel documents**

The Dutch DPA organised an expert meeting in 2006 on the use of biometrics in travel documents. The points that were discussed included usefulness, need and possible disadvantages of the large-scale centralised storage of biometric information. Those present at the meeting pointed out to the government the risks of 'function creep', identity fraud and inadequate security.

> **Citizens Service Number**

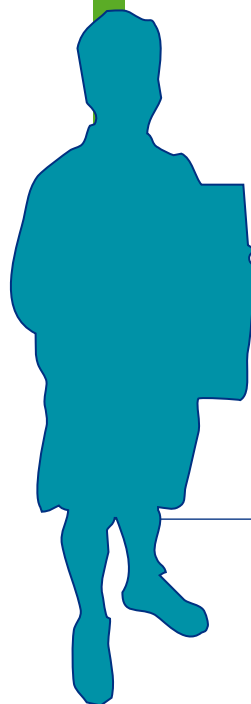
The introduction of the burgerservicenummer (BSN) [Citizens Service Number] has been postponed yet again. The Dutch DPA kept both houses of the Dutch Parliament regularly informed of its positions in relation to some thorny issues associated with this introduction. The Dutch DPA also provided advice on the introduction of the BSN in healthcare, where accurate personal data is sometimes of literally vital importance.

> **Security and privacy**

The research carried out by Prof. H.R.B.M. Kummeling and Prof. E.R. Muller, at the request of the Dutch DPA, the Minister of Justice and the Minister of Interior & Kingdom Relations, which was focussed on finding a proper balance between security and privacy, will result in publication and a congress during 2007.

> ***Wrongly delivered post***

Instead of sending it to the intended local authority, a reintegration bureau sent the progress report on one of its clients to another client. That other client submitted a written complaint to the bureau, having been faced with sensitive personal information relating to someone else. He heard no more about his complaint apart from an acknowledgement of his letter. "It seems as if they don't think this is important", was his response, "although it looks to me like a serious breach of privacy."



ask citizens more than once for information already in its possession. In the opinion it submitted to the Secretary of State for Social Affairs and Employment, the Dutch DPA emphasised the importance of adequate provision of information to the citizen, who must be able to exercise a right to inspect and correct information, as well as the need for transparency. Otherwise, the digital customer file is at risk of becoming primarily a system about instead of for the citizen.

Ten Golden Rules

Are the social services permitted to look at my bank statements and make copies of them? Can they phone up my GP to ask whether I've paid him a visit? Can they act on tips from my neighbours about me? The Dutch DPA regularly sees questions of this sort about the processing of personal data by the social services. With assistance from some employees in a range of social services, the Dutch DPA prepared a brochure in 2006 for the social services, containing answers to these questions. The Ten Golden Rules are designed primarily to provide a practical handbook to the employees who are responsible for intake and for assisting clients.

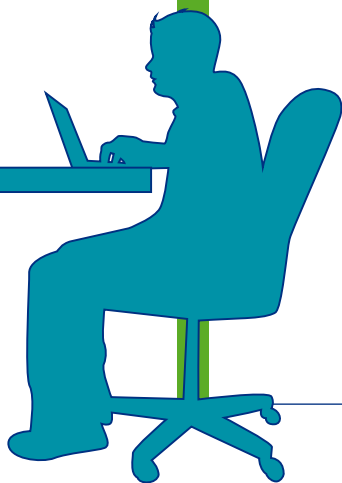
RFID

Radio Frequency Identification is a technology that can be used to implant objects with miniscule chips containing information that can be read remotely. The application of this technology can have great benefits, principally in the area of logistics, but can also be a matter of concern in society. The characteristics of RFID lend themselves to unlimited use of data in a wide range of sectors. The concern arises if, through mass application of this technology by governments and private individuals, people lose control over the data collected in relation to them and subsequently processed and stored in back offices.

RFID poses special problems for compliance with and application of the rules for processing personal data. In order to stimulate public debate on the use of RFID, the Dutch DPA issued a study in 2006 entitled *RFID. Veelbelovend of onverantwoord?* [RFID. Promising or irresponsible?]

> Mistaken identity

When a customer logs on to a website, he is surprised to find not his own details there but those of someone else: login name, date of birth, name and address, e-mail address, social insurance and bank account numbers and annual income. The customer fears that someone else can now see his information, and gets in touch with the web host. The web host checks the customer's information and can put his mind at ease to some extent: his information cannot be viewed by anyone else. An error in the system, however, has allowed him to see someone else's details on his screen. "Unacceptable", as far as the customer is concerned.



Anti-fraud measures and linking files

Not every inhabitant of one of the poorer areas is a potential terrorist, and not everyone entitled to benefit payments is a potential fraudster. Countering abuses in a business by opening up whistleblower lines or introducing black lists is a justified interest, as is the exposure of potential benefit fraud through secret surveillance. But the situation with this type of data processing is that the target interest must be weighed against the impact on the private lives of those on whom the whistle is blown or who are suspected of having acted fraudulently.

Whistleblower lines and black lists

The American Sarbanes-Oxley legislation obliges companies established in the United States to open up internal whistleblower lines throughout their subsidiary companies, with the aim of promoting commercial integrity. This obligation has no statutory basis in the Netherlands, however, even for multinational subsidiaries, that would allow them to set up this type of whistleblower scheme. The governing requirement here is that the company must observe the rules imposed by the Wbp for passing on personal data to countries outside the EU. Because the group-wide whistleblower line is usually set up to provide information to the parent company in the USA, personal data may only be passed on in the event of abuses where it is clear that the report cannot be dealt with properly at a lower level. The Article 29 Working Party has prepared guidelines on the compatibility of whistleblower schemes set up under the Sarbanes-Oxley legislation on the one hand and the EU data protection rules on the other hand. The aim of this is to offer some certainty to companies that are subject to the European data protection rules as well as the Sarbanes-Oxley legislation. Under the guidelines, a permit is required from the Minister of Justice to pass on personal data via the whistleblower line, unless the data is adequately protected in the relevant foreign country.

Another method of countering staff misconduct - ranging from pilfering the petty cash to more serious offences - is the introduction of black lists. For the retail trade sector, which suffers seriously from misconduct, a warning register has been created to store the details of perpetrators who have been charged, and who have therefore been dismissed. Employers can consult the list when recruiting staff to see whether the applicant is included on the list. In the course of 2007, the Dutch DPA will give its definite response to an investigation it has carried out into the practical operation of this type of blacklist.

There is a limit to linking of files

For combating housing fraud by individuals who are in receipt of benefit payments, local authorities can request information relating to their gas, water and electricity usage. One local authority also wanted to link information from waste treatment records with the social services records, to get some indication about the occupancy of a residence. The Dutch DPA considers this is going too far. The local authority was unable to demonstrate that this extra information was necessary, in addition to all of the information already available and the home visits. This type of file linking is also contrary to the finality principle. Citizens are obliged to hand over their household waste and the waste processing company has their information with a view to issuing invoices. The information may not be used for another purpose.

The Internet

The Internet poses a paradox. On the one hand, people are prepared to consign their most intimate information and transactions to the Internet. On the other hand, people can suffer a great deal of damage and grief as a result of their information becoming available on the net.

Objectives 2007

In 2007, the Dutch DPA will place greater emphasis on enforcement by means of investigative research and less emphasis on advising individual parties. The shift towards a greater degree of supervision is required in order to increase awareness of the importance of privacy rules and to improve compliance with them. The proposed investigations will not always be announced in advance, and not all of them are mentioned below.

These are some of the objectives we will be attempting to achieve in the coming year:

- > **Publications on the Internet**
Personal information can now be published via the Internet more easily than ever, and on a wider scale. Such information also remains readily accessible to anyone for years on end. In 2007, the Dutch DPA will publish guidelines on the requirements imposed by the Wbp for this type of publication, and will also carry out some investigations.
- > **The public transport chip card**
There are plans to introduce the OV-chipkaart [public transport chip card] throughout the whole of the Netherlands from 1 January 2009. The Minister of Transport, Public Works and Water Management has promised to do all that is necessary to ensure that the OV chip card system will comply with the Wbp, and is mediating in the debate between the transport companies and the Dutch DPA. The OV chip card will be introduced gradually. The Dutch DPA will accordingly carry out research on one of the systems to be introduced in 2007.
- > **Introduction of electronic patient file**
The Elektronisch Patiëntendossier (EPD) [electronic patient file] is advancing steadily. Access to the data, data and system security and providing accurate information to the patient are important aspects for the patient's privacy. The Dutch DPA will therefore carry out research in one of the regions where the EPD (or elements of it) is being trialled.
- > **Compliance of the Municipal Records Database**
The Gemeentelijke basisadministratie (GBA) [Municipal Records Database] is not transparent as far as most citizens are concerned, while many organisations systematically obtain details of amendments to personal data from the GBA. Research in 2005 into this provision of information to third parties from the GBA showed that those purchasing information did not use different methods for dealing with information marked with a confidentiality indicator and information without any such indicator. The Dutch DPA will carry out investigative research in 2007. Enforcement action will also be taken against local authorities who fail to fulfil the obligation to carry out audits on the GBA.
- > **Combating fraud in social security**
With fraud prevention in the area of social security, the tendency at this point is to carry out large-scale audits. One of the ways this is done is by linking as many files as possible with data concerning large numbers of citizens. While appreciating the need for fraud prevention, the Dutch DPA's principle is that not every individual entitled to benefits should be earmarked in advance as a potential fraudster, and that those citizens who are audited should also be informed of this process. The Dutch DPA will be carrying out investigative research into some of these linkages during 2007.
- > **Computerised student files**
The computerisation of student files is steadily simplifying the exchange of data between the educational sector and other sectors. Student files also contain large amounts of information. It is important for parents to be properly informed about this and for schools to be aware of the rules covering the processing and/or provision of personal data. We shall be emphatically informing the educational sector about these rules during 2007.
- > **Arbodienst [Occupational Health and Safety Service] and ICT**
Investigative research among occupational health and safety services will be carried out during 2007. Collaborative links between these services and insurers are usually also supported by computer (communal data banks, intensive exchange of information). The research will look into whether these relatively new technological developments meet the statutory rules for the processing of personal data.
- > **Privacy rules and the police**
Within the police forces, the functionarissen voor de gegevensbescherming (FG's) [data protection officers] supervise the prudent use of personal data. Citizens can directly contact privacyfunctionarissen (PF's) [privacy officers] of the various forces with any questions, complaints or requests to find out about their information. In the interest of unambiguous and uniform processing of data by the police, the Dutch DPA will pay extra attention during 2007 to the relationship with both of these categories of officers.

> **Surveillance society**

An increasing part is being played in society by information systems that allow close following and checking of individuals, as well as systems intended specifically as instruments of supervision (including cameras linked to recognition systems, chips in smartcards, GPS, and the recording of telephone data). If a surveillance society seems unavoidable, then at the very least we have to be aware of the risks that the mass application of information technology poses. In 2007, the Dutch DPA will make sure that these developments are not lost sight of.

> **Collaboration with other supervisory authorities**

Closer collaboration will be sought with other supervisory agencies during 2007. The Dutch DPA will conclude a co-operative agreement with the Nederlandse Zorgautoriteit [Netherlands Healthcare Authority]. The joint investigation prepared in 2006 by the Inspectie Gezondheidszorg [Healthcare Inspectorate] and the Dutch DPA into the protection of information at hospitals, will be carried out during 2007 as well as an investigation, in collaboration with the Inspectie Werk en Inkomen [Inspection Work and Income], into the processing of personal data in buildings that house several businesses for public and private parties (CWI, Sociale Dienst [Social Services], UWV, reintegration agencies.).

> **Wbp case law**

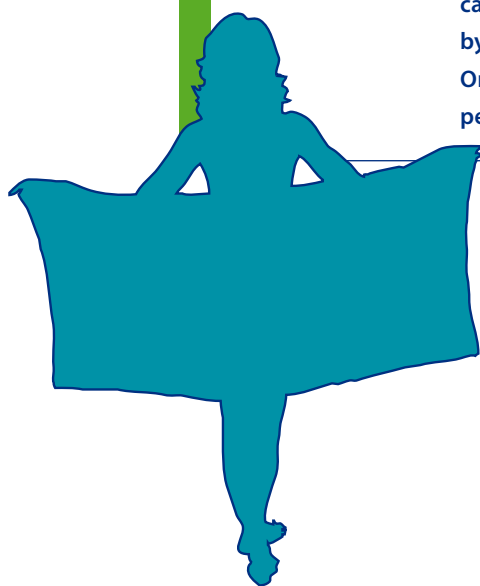
A collection of opinions issued by the Dutch DPA, based on the Wbp, will be produced in 2007. This book is a sequel to the 1999 publication entitled *Persoonsgegevens beschermd* [Personal data protected], which was devoted to judgments based on the Wet persoonsregistraties (WPR) [the previous Data Protection Act]. It also includes pronouncements by dispute committees and the courts that are of major significance to the practice of the law. Collating the folder is a joint project with the Duthler advisory bureau. Two independent academic lawyers will act as editors, namely Prof. D.W.F. Verkade and Prof. H.Ph.J.A.M. Hennekens.

Publications on the Internet

The Dutch DPA commenced a project in 2005 to list the privacy problems experienced by citizens in their day-to-day lives from publications on the Internet. From the start, the issue of what should and should not be authorised as regards processing of personal data on websites was clearly very complex. The Dutch DPA set a target for itself in 2006 of developing a provisional policy that would serve as a prompt for further discussion on this topic. This policy suggestion was set out in a preliminary report presented during a symposium held to mark the occasion of J.W. Broekema leaving the Authority. The Dutch DPA will publish guidelines in 2007 for dealing with personal data in publications on Internet.

> *Camera supervision in shower rooms*

The management of a 24-hour business wants to set up cameras in the shower rooms and changing rooms used by its terminal staff, so as to be able to monitor them. One of the employees wonders whether this is, in fact, permissible.



The use of personalised services on the Internet, such as G-mail, leaves the providers of these services with ever larger 'data warehouses', containing personal information such as search instructions, the contents of e-mails or even the contents of the whole hard disk of a computer. Making this information available to third parties can cause serious problems to Internet users.

At a one-day debate on 7 December 2006, organised by the Dutch DPA and the Consumentenbond [Dutch Consumer Association], Google Europe acknowledged that IP addresses, the numbers used to identify computers, amount to personal data in many cases and are accordingly entirely subject to the statutory protection of personal data. The Dutch DPA emphasised the importance of Internet users receiving sufficient information from the service providers, that their information should not be used haphazardly in a different context, that everyone should be able to inspect and if necessary correct their own information, and that there should be a maximum time limit for storing information.

Opening up archives

Digitising and opening up existing archives - not including modern digital weblogs and suchlike - to a wider public is considered to be important, and is also promoted by the government. Because archives can contain specific personal data, it is important to set up rules of play for unlocking and digitising existing archive material, based on the requirements of the Wbp. The Dutch DPA has issued an opinion on this for the national heritage sector. Online archives containing personal data must be reported to the Dutch DPA or the data protection officer if the heritage institution has appointed this type of supervisor.

Opening up archives via the Internet merits special attention. The unusual thing about unlimited provision of information via the Internet is that personal information is made available to everyone throughout the world, without any time restriction. Those responsible do not know who will be receiving the personal information. It is doubtful whether they are acting with due care by doing this. In any case, they cannot hide behind any statutory duty, as there is no statutory obligation to publish personal information via the Internet.

Education and study

Information concerning parents and students

In March 2006, the Dutch DPA submitted its legislative opinion to the Minister of Education, Culture and Science in connection with the Ministry's new weighting scheme for elementary school budgets. Under the new budgeting system for dealing with educational disadvantages, the extra funds are allocated in principle on the basis of parental education levels. The Dutch DPA advised the Minister to use the explanatory memorandum for the Bill to devote specific attention to the interests involved in processing parental information.

In July 2006, the Dutch DPA was approached by parents who had taken their child's school brochure to mean that they were obliged to provide information on their own levels of education. There is no such obligation, however. In an independent advisory note of 20 July 2006, the Dutch DPA suggested to the Minister that he should publish information - via the Ministry's own Cfi website and also through other available channels such as school boards and directorates - to the effect that there was no such obligation incumbent on parents. The Minister informed the Dutch DPA that the suggestion would be taken on board. The text of the parental declaration has been amended to make it clear that parents are not obliged to complete these details. The text of the explanatory brochure will also be adjusted in a future edition.

Exchange of information for professions or study

The Dutch DPA considers that the Bill proposed by the government for translating the EU directive on recognising vocational qualifications into Dutch law should not be submitted in its present format. There is no doubt that the recognition procedure requires an exchange of personal information, but the Bill is so vague that it would be completely unclear to the citizen what information would be involved.

Studying abroad is becoming more and more popular. It is going to become possible to use student funding in many more countries than is presently the case. An exchange of information with the authorities in other countries is required to check on student finance arrangements. The Dutch DPA has indicated to the Secretary of State for Education, Culture and Science that there is a need to exercise caution when passing on particular information to countries outside the European Union, if such information might have unintended negative consequences for the student, such as information on cohabitation arrangements.

Summary of investigations carried out in 2006

Europol

In 2006, the Dutch DPA again took part in the annual audit of the Europol systems by the Joint Supervisory Body of Europol. These audits regularly show the great importance of the member states supplying high-quality information. In addition to the quality of information, the investigation also looked at whether the information system was operating in accordance with the Europol agreement. The audit in 2006 also investigated how far the recommendations for improving Europol's internal organisation, made in 2004 and 2005, had been implemented. The inspection showed that Europol had implemented most of the points for improvement disclosed by earlier audit investigations.

Eurodac

Eurodac is an EU-wide system for comparing fingerprints taken from foreign nationals. The database is based on a hit/no hit system: member states take fingerprints from asylum seekers and illegal immigrants found in their countries and then compare these with the data present in the system in order to establish which member state is responsible for dealing with the asylum application in accordance with the Dublin Convention. The Dutch DPA, one of whose tasks is to supervise national processing of personal data for Eurodac, carried out an investigation in 2006 at the request of the European Data Protection Authority as part of a co-ordinated audit in the various member states. An overall report on the findings, in the European context, is expected to appear during the course of 2007.

Sociale recherche [Social Security Fraud Department]

Through covert observation, the sociale recherche checks on whether individuals in receipt of benefit payments are acting fraudulently. The Dutch DPA approved the procedural description for these observations in 2003. An important element of this is that the citizens who are being checked should be made aware of the fact. Audit investigation during 2006 showed that there is room for improvement in meeting this duty of information.

Destruction of taped conversations with confidants

Investigation was carried out between June 2005 and December 2006 into compliance by the police with the rules for destruction of recorded telephone conversations with confidants such as doctors, lawyers, notaries and spiritual counsellors.

The results of this investigation prompted the Dutch DPA to follow up on the investigation. The Dutch DPA will accordingly carry out a further audit in the first half of 2007 into compliance with the duty of destruction in relation to recorded telecommunications with confidants. The results of this investigation are expected to be published in 2007.

Special Investigation Services

As part of its systematic supervision of the processing of personal data by Criminele Inlichtingen Eenheden (CIE's) [Criminal Investigation Units], the Dutch DPA completed its investigations at the CIE's of two Bijzondere Opsporingsdiensten [Special Investigation Services] in 2006. No data was found at the CIE's in question that ought not to have been processed by those CIE's. In relation to organisational and technical aspects, and just as with the earlier investigations at CIE's carried out in 2003/2004, the Dutch DPA brought some matters to the attention of the responsible Ministers that would benefit from improvement.

Private detective agencies

2006 saw the publication of the results of an investigation carried out in 2005 into compliance by private detective agencies with a number of standards under the Wbp. The main standard involved here was compliance with the obligation to provide information. It turned out that, in a large number of cases, the agencies did not know whether they had fulfilled this, having left it to their client to inform the individual under investigation and not having checked whether the client had actually done so. Virtually none of the agencies had prepared any working instructions or procedures regarding this process. The Dutch DPA considers it necessary for agencies to regulate compliance with the duty to provide information with their clients in writing.

Black lists in the retail trade

Members of staff who are charged with theft or fraud, and who are then dismissed, can have their names placed on a blacklist. Employers can consult the list in order to screen job applicants. The Dutch DPA carried out research during 2006 into the operation of this 'warning register' in the retail trade, in order to check whether the system was operating in accordance with the Wbp and the Protocol for the warning register. The results will be published in 2007.

Financial service providers

The Dutch DPA considers careful processing of personal data to be of great importance in the financial sector. Compliance with the Privacygedragscode Financiële Instellingen [Privacy Code of Conduct for Financial Institutions] was investigated in 2006. The aim of the investigation was to gain some understanding of compliance with the requirements set out in the Wbp and the Code of Conduct. The results of the investigation are expected in 2007.

Healthcare insurers

The European national supervisory authorities, in the context of their work in the EU Article 29 Working Party, resolved to carry out coordinated research into the processing of personal data in the health care insurance sector. The investigation is intended to reflect the state of affairs across Europe as regards compliance with privacy legislation in the sector. The research was carried out between April and October 2006. It is expected that results will be published in mid-2007.

> A 'rogues' gallery

"They want to set up a 'rogues' gallery' at our company. This is because we recently had a merger and people don't know each other. They want to put our names and jobs beside the photographs. Can they just do this? Can they force me to do this? Or do you need permission from every employee?"

