2007 summarised

Compliance with the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act] is not only in the interest of individual citizens. Respect for individual privacy also serves a collective interest: a society in which we can assume that our personal data will not be misused, making it possible to trust the government, companies, institutions and each other. In 2007, in order to make a stronger and more visible contribution to the protection of this collective interest, the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] decided to place more emphasis on the use of supervisory investigations for the enforcement of statutory rules in its work. Priority is being given to dealing with serious violations of a structural nature, with an adverse impact on large groups of citizens. Through the enrichment and broadening of general information on the Dutch DPA website, citizens are encouraged and helped to resolve their problems themselves and also, where necessary, to take action themselves.

Large-scale data collection and processing was high on the agenda of the Dutch DPA in 2007, just as it has been in other years. At a European level, areas of concern included the collection of data on passengers flying from Europe to the United States and on passengers within the EU. At a national level, privacy problems in relation to the OV- chipkaart (digital transport pass) and the Elektronisch Patiëntendossier (electronic patient file) are salient issues. These and other subjects will be discussed briefly below in a selection from the activities undertaken in 2007.

International collaboration

The Dutch DPA co-operates with other national data protection authorities at a European and international level. At a European level, the Netherlands plays an active role in the working group of EU data protection authorities, the so-called Article 29 Working Party (WP29). In 2007, the WP29 had serious discussions on the proposal by the European Commission, which followed the PNR agreement with the United States, to collect passenger data within the EU as well, with the object of combating international crime and terrorism. Jacob Kohnstamm, Chairman of the Dutch DPA, stated that this was contrary to Article 8 of the ECHR.

News can also be reported in the field of financial data traffic. More in particular, this concerns SWIFT, the company that facilitates international transfers for banks. In 2007, reports in the media made it clear that SWIFT stores back-up data on account holders in the United States and that the authorities in the US can demand access to these data. Contrary to their obligation in this respect, banks had not informed their customers of this fact. Following the threat of enforcement by the Dutch DPA, banks in the Netherlands finally decided to inform their account holders of the transfer of their data. In a WP29 context, following coordinated action by all national data protection authorities, SWIFT indicated that it will open a data storage office in Switzerland in 2009, as such resolving the problem of the provision of data on intereuropean transfers to the US.

In terms of police and the judicial authorities, the European supervisory authorities point to the ongoing need for a high level of protection for personal data exchanges for investigation purposes.

The Dutch DPA regularly takes part in the joint supervisory data protection authority activities at a European Union level, in relation to collaboration between the police and judicial authorities.

National collaboration

Co-operation with other supervisory authorities and organisations involved in data processing leads to more efficient supervision of compliance with the statutory rules that protect personal data, and also contributes to the broadening of support for privacy protection.

In April 2007, the Dutch DPA worked with the Inspectie jeugdzorg [Youth Care Inspectorate] to organise a round table conference on the obstacles that privacy legislation would create for the exchange of data by welfare agencies in the battle against child abuse. It was found that there were not actually any obstacles. This shared view on the part of representatives of a large

number of professional parties involved in the field of youth care was communicated to the Minister for Youth and Family, linked to proposals for the exchange of data that can make a fundamental contribution to efforts to combat child abuse.

As regards the processing of personal data in the healthcare sector, delineation agreements were made with the Nederlandse Zorgautoriteit [Dutch Care Authority] and an investigation was conducted into the protection of patient data together with the Inspectie voor de Gezondheidszorg [Healthcare Inspectorate].

Other joint projects in 2007 involved the retention obligation for traffic data, the use of the burgerservicenummer (BSN) [citizens service number] by the business sector and the joint use of personal data by the Centrum voor Werk en Inkomen (CWI) [Centre for Work and Income], the UWV [a body implementing employee insurance schemes] and municipalities. In 2007, the network of functionarissen voor de gegevensbescherming (FGs) (data protection officers), the independent internal regulator for companies and organisations, was further expanded. The Dutch DPA has an annual meeting with the professional organisation for FGs.
In the process initiated in 2006 by the Dutch Parliament, the object of which is to create a National Institute of Human Rights: in April 2007, the four organisations that would participate in this institute published a memorandum on how the organisation could be launched. The Minister of the Interior and Kingdom Relations has not decided on this proposal yet.

Public administration

The BSN [citizens service number] was introduced at the end of November 2007. This marks the start of a new phase for the Dutch DPA. At the BSN management facility, a personal public service point will be created, which local authorities and citizens can approach with any questions they may have. As the authority responsible for supervision of the careful handling of personal data, the Dutch DPA is the authority with competence to intervene in the event of real problems with implementation of the Act.

The Gemeentelijke Basisadministratie (GBA) [municipal personal records database] contains the personal data of all individuals registered in a specific municipality. This administration forms the basis for the implementation of many government tasks. It is very important that data are correct and that they are protected properly. The municipalities are obliged to perform audits once every three years. Following the announcement by the Dutch DPA that it would take enforcement action where municipalities failed to fulfil their audit obligation, or failed to do so on time, an improvement in municipality compliance with the statutory obligation applicable was observed in 2007 in comparison with previous years. Last year, the Dutch DPA imposed an order for periodic penalty payments on four municipalities.

At the end of 2007, at the request of the Senate, the Dutch DPA issued advice on a legislative proposal that would extend the powers that the intelligence and security services, in their efforts to combat terrorism, have in obtaining data on travelling, payment traffic and Internet use by citizens. The Dutch DPA believes that the need for these measures in addition to the many measures already in existence has not been demonstrated and considers that the consequences of this data analysis for individual citizens, but also for responsible parties and the services involved, have not (or not sufficiently) been recognised.

The Dutch DPA also expressed its criticism of the proposal for a verwijsindex risicojongeren (VIR) (national reference index of young people at risk). The Dutch DPA agrees wholeheartedly with efforts to achieve better and faster help for children and young people with problems, but it is not yet clear whether the sole objective of the reference index is the provision of assistance, or whether its aim is also to help maintain public order. Complete clarity about key terms and criteria is necessary.

Police and the judicial authorities

Safety and privacy are both vital for citizens. However, all too often in public debate, these values are, rather simplistically, construed as opposing values. To help put the discussion back on course, the Dutch DPA, in collaboration with the Ministry of Justice and the Ministry of the Interior and Kingdom Relations, commissioned research into the identification of the most appropriate balance between the efforts to achieve a safe society and the efforts to safeguard the right to privacy. The resulting external research report, with guidelines for more effective dialogue, was presented at a symposium on 1 November 2007.

In situations where the police tap telephone calls in the context of criminal investigations, conversations between lawyers and their clients are often recorded too. These conversations with holders of confidential information entitled to privilege must be erased as soon as possible. A Dutch DPA investigation of the national wiretapping rooms shows that this does not happen correctly or on time in far from all cases. The Public Prosecution Service has announced that measures for the improvement of this situation will be implemented.

In recommendations on proposed new legislation, or other regulations in the field of criminal law, the Dutch DPA regularly raises the following question: has it been demonstrated that the regulations in question are really necessary? Is it clear that existing or previously proposed statutory possibilities fall short? For example, in the opinion of the Dutch DPA, in the light of improved identification possibilities in the future, the Minister of Justice has provided insufficient justification for the proposal for a central database for the storage of the identity of all suspects and convicted offenders. And do the plans by the police, the Public Prosecutions Department and the Koninklijke Marechaussee (KMar) [Royal Netherlands Military Constabulary] to record the registration number of all motorists entering Amsterdam via the Utrechtse brug, regardless of whether they have a clean record or not, really contribute to a safer society?

Work and social security

Citizens do not automatically become suspects simply because they receive benefit or housing benefit. In the 'Waterproof' project, old-age pensioners and recipients of a social assistance benefit in 65 municipalities in Friesland, Groningen and Drenthe were checked for fraud based on data on their water consumption and the water contamination surcharge. The data obtained were also used to check fraud with housing benefit. The Dutch DPA investigated this linking of computer files and ruled it unlawful. It is important to combat benefit fraud, but monitoring based on the linking of computer files is only permitted on the basis of sound risk analysis, since this makes it possible to show that it is necessary to further monitor a group of citizens at a high risk of entering the fraud zone. As a result of the Dutch DPA ruling, the Sociale

Inlichtingen- en Opsporingsdienst (SIOD) [Social Security and Investigation Service] is now working on the development of risk analyses using Privacy Enhancing Technology (PET). In this way combating fraud and the protection of personal data seem to be able to go hand in hand.

Another way of uncovering benefit fraud is covert observation by social security investigators. The processing method used for the personal data connected with these activities has been laid down in a process description approved by the Dutch DPA. Research in 2006 showed that compliance with the obligation to inform citizens of the fact that they had been observed left something to be desired. The process description was then tightened up in 2007.

In the event of a transition to a occupational health and safety service provider, can the former service provider transfer employees' records to the new service provider without this being provided for by law? The Dutch DPA ruled 'no' in 2006. Further to indications from the field that this view caused problems, the Dutch DPA did research in 2007 to ascertain whether a different approach is possible within the existing statutory frameworks. This led to an outcome whereby transfers were made subject to a distinction between data that are not subject to medical professional secrecy and data that are. In the first case, the data may be transferred. In the second case, data may only be transferred under certain conditions.

The Dutch DPA also examined the standard provision of data by the UWV to all current employers on the occupational disability history of a new employee, as a result of which the UWV will now only do this where the employer in question has a specific, direct and vested interest in doing so.

Healthcare

The Dutch DPA issued a critical advice on a draft legislative proposal that provides for the introduction of an electronic patient file. In the opinion of the Dutch DPA, making patient files available to all care providers is far too risky, partly with a view to the protection required for particularly sensitive personal data. With the exception of emergency situations, only care providers with a treatment relationship with a patient ought to have access to the record in question. If this is not the case, there is a risk that unauthorised parties will misuse or misappropriate the medical data.

In 2007, the Dutch DPA also issued a negative advice on making the elektronisch kinddossier jeugdgezondheidzorg (electronic child record for the youth healthcare sector) compulsory in the legislative proposal that relates to youth healthcare and infectious diseases. The need for the central electronic storage of data had not been substantiated sufficiently. The Cabinet has since said that it is no longer seeking to create a central electronic child record and that it is looking for other ways to exchange communications in the youth healthcare sector.

The Dutch DPA has made agreements with the Minister for Health, Welfare and Sport on the application of Privacy Enhancing Technologies when using data in the DBC information system and for the purpose of risk equalisation in the context of the Zorgverzekeringswet (Zvw) [Health Care Insurance Act].

Trade and services

Following the announcement by the Dutch DPA that it would take enforcement action against the unlawful combined storage of the name and address details of travellers and their travel data, the public transport companies would seem to have finally recognised that the OV-chipkaart has side effects that are contrary to the Wbp. In 2007, in a pilot on the Amsterdam metro network, research was done into the impact of the card, which ended with the conclusion that the OV-chipkaart system is being used unlawfully. The Gemeentevervoerbedrijf (GVB) [Municipal Transport Authority] and other public transport companies have now undertaken to bring practice in line with the Wbp. In the technical design for data storage, a distinction will be made between name and address details on the one hand and travel movements on the other hand. As a result, the risk of the unlawful monitoring of individual people's travel behaviour will be limited considerably.

In 2004, the Stichting Fraude Aanpak Detailhandel (FAD) created an alert system consisting of a central database – a black list – containing the personal data of all members of staff who have committed serious offences. Employers can consult this database before employing an applicant. The Dutch DPA approved this objective. In 2007, an investigation was conducted into the impact of this system. Amongst other things, this investigation showed – entirely contrary to the boundaries indicated by the FAD itself at the time – that not only individuals who had committed serious offences had been entered onto the database, but also many – often young – employees who were guilty of relatively minor offences. In many cases, these individuals had not been informed of their registration either. The Dutch DPA issued an announcement for enforcement action, in order to ensure that the alert system will be used in accordance with the information provided by FAD in 2004 and the protocol approved on this basis.

Further actions by the Dutch DPA concerned a very wide range of different subjects: camera surveillance in changing rooms at swimming pools, the registration of hotel guests, the permanent screening of legal entities, compliance with the obligation to disclose information by private detective agencies and the provision of personal data to countries without a sufficient level of protection.

The Internet

Personal data are published on the Internet in a large number of different ways and are generally accessible worldwide, 24 hours a day, for an extensive and diverse public. There can be unexpectedly serious consequences for Internet users – amongst whom are many children – whose personal data are on the web. In 2007, the Dutch DPA developed and published guidelines in order to clarify what is permitted and what is not when publishing personal data on the Internet. The individuals responsible can use these guidelines to assess whether publication of personal data on the Internet is permitted. A large amount of information material has also been published on the Dutch DPA site. As regards minors, the Dutch DPA takes a proactive stance in providing the rules applicable for social networks and for online marketing.

The government also makes use of the Internet. In 2007, the Dutch DPA conducted an investigation into how the municipality of Nijmegen publishes data on planning permission. Complete scanned copies of application forms were published on the net, containing not only

data on the property in question and on the alterations proposed, but also personal data on the applicant, including his/her signature. In the opinion of the Dutch DPA, the municipality must only publish compulsory data on the Internet – on the property in question and the alterations proposed.

The proper performance of a public-law task does not justify a situation where an administrative body automatically publishes all data on the Internet. The Dutch DPA will also publish guidelines on the privacy aspects of active public disclosure in the framework of the Wet openbaarheid van bestuur (Wob) [Government Information (Public Access) Act] in 2008.