

# Review of 2005

According to public opinion, it has become evident over the past few years that the protection of personal privacy is no longer a foregone conclusion. Concerns about terrorism, insecurity and social wrongdoings on the part of citizens, administrators, politicians and policy-makers have resulted in the regulations for personal data protection being used in the public debate as a scapegoat or denounced as an obstacle. In addition to the socio-political climate, the surveillance domain is also subject to radical changes. Therefore, in 2005 the Dutch Data Protection Authority (Dutch DPA) [College Bescherming Persoonsgegevens] expressly posed the question as to what essentially the WBP [Dutch Data Protection Act] should serve to protect and the path that must be taken in order to achieve this. In these changing times, the power of expression of the law is becoming less dependable and greater use must be made of the visions and findings of others. The Dutch DPA considers itself fortunate that in 2005 – and also in the context of the forthcoming evaluation of the WBP – it was able to rely upon the willingness of many discussion partners, including academics, experts in the field, companies and social organisations, to contribute their ideas in this regard.

Monitoring compliance is the most important task that the legislator requires of a supervisory authority. Effective supervision of compliance with and, where necessary, enforcement of the regulations with regard to handling personal data is essential. However, there are insufficient people and resources available to be able to carry out this task to full scale. In recent times, the Dutch DPA has been unable to contribute, or has only been able to contribute to a limited extent, with regard to all kinds of issues. The shift in policy desired on a social and political level towards more inspections and greater enforcement could only be partially achieved. The Dutch DPA has had to pull out all the stops at least in a few large cases to do what had to be done in view of the inherent risks to the protection of personal privacy.

## Healthcare systems

The change in the healthcare system gave the Dutch DPA a reason for intensive involvement. After the advice obtained in 2004 with regard to the *Zorgverzekeringswet (Zvw)* [Healthcare Insurance Act], in 2005 the Dutch DPA paid much attention to the elaboration of the system change. Agreements have been made with the Minister of Health, Welfare and Sport as to how the shortcomings in the Zvw in relation to the processing of personal data can best be resolved. To this end, Article 87 of the Zvw amongst other things, has, in close consultation with the Dutch DPA, been elaborated in a ministerial order, the *Regeling Zorgverzekering* [Health Insurance Order]. It has been further agreed that the 'service descriptions', which largely form the content of the flow of information between healthcare practitioners and health insurers, will be determined by the Healthcare Authority in consultation with the Dutch DPA. The service descriptions indicate in detail which personal data must be provided for the purpose of invoicing for the healthcare provided.

### Risk equalisation

It has also been agreed with the Minister of Health, Welfare and Sport that no personal data will be used for risk equalisation. It will suffice to use pseudonymous data, i.e. the data are linked to a unique but anonymous code. The Dutch DPA also advised that a number of preconditions be laid down in the ministerial order building upon Article 35 of the Zvw relating to the processing of personal data for the purpose of risk equalisation. During the transition to the system under the Zvw, personal data were temporarily necessary (only for the ex-ante calculation 2006). The temporary nature of this processing has been established as well as a maximum storage time for the required data.

### Healthcare Insurers' Addendum to the Code of Conduct

The Healthcare Insurers' Addendum, drawn up by *Zorgverzekeraars Nederland (ZN)* [Association of Dutch Healthcare Insurers] contains rules of conduct with regard to the processing of personal data by health insurers and is an addition to the existing *Gedragscode verwerking persoonsgegevens financiële instellingen* [Code of Conduct for Financial Institutions] with regard to the Processing of Personal Data. Amongst other things, the Addendum contains rules in relation to handling invoice data and performing substantive checks on invoices.

Intensive discussions between ZN, the Ministry of Health, Welfare and Sport, the KNMG [Royal Dutch Society for the Advancement of Medicine] and the *Nederlandse Patiënten Consumenten Federatie* [Dutch Patient Consumer Federation] and the Dutch DPA resulted in agreement on the content of this appendix at the end of 2005. The Dutch DPA declared its approval of the Appendix in accordance with Article 25 of the WBP in April 2006.

### **Diagnosis Treatment Combination and DTC Information System**

The agreement with the Ministry of Health, Welfare and Sport and ZN to make the *Diagnose Behandeling Combinaties (DBC's)* [Diagnosis Treatment Combinations] less detailed and privacy-sensitive as possible unfortunately no longer appeared to be on the agenda in 2005. This means that as of 2006, DBC's with detailed information that is subject to doctor-patient confidentiality will be passed on to healthcare insurers by healthcare practitioners in hospitals. The Ministry has promised the Dutch DPA that the DBC system will be simplified in the coming years.

Agreements have been made with the Minister of Health, Welfare and Sport on the application of Privacy Enhancing Technologies (PET) in using data in the DBC information system (DIS). The DIS is a large databank, a national interchange for receiving, processing and issuing data that are provided by hospitals and medical specialists. By implementing this technical solution, the identity of the individuals behind the data can remain anonymous. This does not detract from the fact that the DIS, as far as scale, coverage and content is concerned, will be one of the highest risk processing systems in the Netherlands.

### **Mental Healthcare**

As of 2007, a large part of mental healthcare will be paid for via the Zvw. Mental healthcare currently still falls within the remit of the *Algemene wet bijzondere ziektekosten* [Exceptional Medical Services Act]. The intention is to bring mental healthcare aimed at 'recovery' under the Zvw. DBC's will therefore also be introduced in mental healthcare as of 2007. In consultation with the other groups in the profession, in 2005 the Dutch DPA expressly requested that attention be paid to the protection of personal data in this field.

### **Law on the Use of the Citizens Service Number in the Healthcare sector**

With effect from the entry into force of the *Wet algemene bepalingen burgerservicenummer* [General Provisions on the Citizens Service Number Act], the current 'sofi-number' will be used under the name of *burgerservicenummer (BSN)* [Citizens Service Number] by and for all communication with the (semi-) public authorities. The *Wet gebruik burgerservicenummer in de zorg* [Law on the Use of the Citizens Service Number in the Healthcare sector] stipulates that healthcare providers, healthcare insurers and indication bodies will have to use the BSN in exchanges of communication relating to patients. The BSN will also be used in the future to make the Electronic Medication File and the Electronic Patient File possible. The Dutch DPA was highly critical of this draft bill. The introduction of such a unique identifying number indeed carries high risks, risks that must in any case be limited. The bill that was finally presented to the Lower House fell short of the mark in this regard.

## Results 2005

THE PREVIOUS ANNUAL REPORT ANNOUNCED THAT THE FOLLOWING RESULTS WOULD BE PURSUED IN 2005. EARLY 2005, WE WERE FORCED TO DECIDE TO DELAY THE ANNUAL PLAN UNTIL MID-2006.

### • Safety and privacy

In 2004, the Dutch Data Protection Authority (Dutch DPA) issued advice on the legislative proposal concept to extend the possibilities of investigating terrorist crimes. This advice was largely ignored. In 2005, the Dutch DPA brought its advice to the attention of the permanent committee for the Ministry of Justice in the Lower House. At the request of the Lower House, the Dutch DPA has analysed the set-up of the Counter-Terrorism-Infobox (CT Infobox).

Furthermore, the Dutch DPA, in consultation with the Ministries of Foreign Affairs and Justice, has requested professors H.R.B.M. Kummeling and E.R. Muller, to study the balance between safety and privacy. The final report is expected to be published in 2006.

### • Special police registers

In the autumn of 2005, within the framework of structural supervision of the special police registers, the Dutch DPA investigated two special investigation services. The results thereof shall be available in 2006.

### • Risk selection

In 2005, an expert's meeting on risk selection was organised. A publication thereof shall be issued in 2006.

### • Internet and privacy

In 2005, an expert's meeting on the Internet and the protection of personal data was held. An exploration in this field shall be published in 2006.

### • Obligation to provide information

Information activities on the obligation of data controllers to provide information have been intensified. Furthermore, a number of surveys into the compliance with the obligation to provide information were started in 2005 and are scheduled for publication in 2006.

### • Investigating compliance with obligation to notify

In 2005, the annual investigations into the compliance with the obligation to notify were prepared, but ultimately not carried out. The delay of the annual plan caused the start of the investigations to be postponed. Ultimately, following the decision of the *Raad van State* [Council of State] (ruling of 21 September 2005, 200504372/1: no basis for fine regarding failure to report processing activities started prior to 1 September 2001), the 2005 series of studies into the obligation to notify were cancelled. The WBP (Dutch Data Protection Act) shall be amended on this point in 2006.

### • Administrative burdens

Following on from proposals made at the end of 2004, the Dutch DPA has held various consultations with the Ministry of Justice and the *VNO-NCW* [Confederation of Netherlands Industry and Employers], which included the subject of extending the exemption of the obligation to notify. Ultimately it is the Minister of Justice who must submit a proposal to the Lower House. In 2005, this had yet to be done.

### • Binding Corporate Rules

The Dutch DPA has made an active contribution to the simplification of the rules for transferring personal data to data controllers outside the European Union. In 2005, the Data Protection Authorities collaborating in the Article 29 Working Party entered into European agreements regarding a uniform procedure for the application of permits and on the coordinated processing of permit applications on the basis of so-called Binding Corporate Rules (BCRs).

### • Collaboration and exchanging personal data

On several occasions in 2005, the Dutch DPA made contributions to clarify regulations in respect of the necessary exchange of personal data among organisations formally collaborating to address particular social problems. In April 2005, the Dutch DPA organised a symposium on this subject. Special meetings aimed at supervising authorities were not organised.

### • Supervision and regulators

In 2005, together with the *Commissie gelijke behandeling* [Equal Treatment Commission], the National Ombudsman and the *Studie- en informatiecentrum mensenrechten* [Netherlands Institute of Human Rights], the Dutch DPA issued advice to the Government on the desirability of setting up a national institute of human rights. In that same year, collaboration agreements were entered into with the *OPTA* [Independent Post and Telecommunications Authority] and the *IWI* [Work and Income Inspectorate].

The number of data protection officers showed a slight increase in 2005.

### • Health Care and Social Security

In 2005, the *Zorgverzekeringswet* [Health Care Insurance Act] was a major issue for the Dutch DPA. The Act and all the changes involved with it, as well as the plans for the implementation of the *burgerservicenummer* [Citizens Service Number] in the healthcare sector required much attention. Furthermore, an explorative study into data flows for reintegration purposes and the exchange of medical data between concern units was carried out among insurers. The publication of a normative framework for the social services shall be published in 2006.

### • Citizens Service Number

As early as 2004, the Dutch DPA issued advice on the legislative proposal for general provisions to implement and to use the *burgerservicenummer* [Citizens Service Number]. The legislative proposal, as submitted to the Lower House in 2005, takes insufficient account of the objections by the Dutch DPA. The Dutch DPA has expressed its concern in respect of this to the Lower House. The intended preparation for the tasks the Dutch DPA would be allocated within the framework of a national ombudsman role has not yet begun due to the delay in the Act coming into force.

### • Evaluation of the WBP

The Dutch DPA has been preparing for the evaluation of the WBP (Dutch Data Protection Act) in various ways, which is expected to take place in 2006 (article 80 of the WBP). Preparations include a number of meetings with field experts and consultations with the Ministry of Justice.

## Terrorism and security

Due to the increase in plans and measures at European level to improve security and to combat crime and terrorism, the exchange of data on suspects and unsuspected persons between the member states of the European Union will become even greater. For this reason, the importance of a harmonised and efficient framework for the protection of personal data for the international exchange of data in the fields of justice and the interior, the so-called third pillar of the European Union, is also increasing.

### Supervisory authority for the third pillar

The spring conference of European Data Protection Authorities in Cracow in April 2005 expressed its approval of the plan of the European Commission to develop a new legal framework for data protection in the third pillar. The high level of protection of the general privacy Directive 95/46/EC is to be the starting point in this regard. It was also argued that an independent supervisory and advice body should be set up in which the data protection authorities would work together. Now that the Constitutional Treaty has not been adopted, the pillar structure of the European Union will remain in place for the time being. This is why in addition to the Article 29 Working Party for the first pillar, such a body is also necessary for the third pillar. In the course of 2005, the European data protection authorities drew up a more detailed recommendation, which was offered to the European Council and the European Commission at the beginning of 2006.

### The Hague Programme

The so-called The Hague Programme, a long-term programme that was defined during the Netherlands' Presidency of the European Union during the second half of 2004, incorporates proposals that are aimed at combating terrorism and cross-border criminality, both within the remit of the third pillar as well as within that of the first pillar of the EU, the internal market.

The most important proposals in 2005 embraced the framework decision on data protection, which falls within the third pillar, the ongoing development of existing European information systems, the effort to ensure improved interoperability and synergy between European databases, the introduction of biometrics in passports and the central storage of data, including visa information. Subsequently, the Directive was implemented that laid down an obligation to preserve data relating to telecommunications traffic.

The proposal for a framework decision with regard to the principle of the availability of police data is far-reaching. On this basis additional data from the Police or judicial authorities can be exchanged between member states. Enforcement data that are available in one member State would then be directly available to other member states. In 2005, the European data protection authorities declared in Wroclaw, Poland that the principle of the availability of enforcement data should only be allowed to be implemented, on condition that a harmonised and sufficient framework for data protection is in place throughout the EU as a whole.

### Powers relating to the detection of terrorist acts

In 2004, the Dutch DPA issued recommendations as to the draft legislation to extend the ability to detect terrorist crimes. Many of the points contained in these recommendations

were not followed up. In 2005, the Dutch DPA therefore brought its criticisms to the attention of the standing committee for Justice in the Lower House of the Dutch Parliament.

The intention of the draft law was to enable the Police to examine all possible indications of terrorism. In the opinion of the Dutch DPA, this is the exclusive task of the AIVD [National Intelligence and Security Service], as the AIVD is ideally equipped for that task and because the intelligence work carried out by the AIVD has been granted considerable protection. If the police has a genuine need to be granted such far-reaching powers, it will also be necessary for adequate guarantees to be put in place. The draft law falls short in this regard, as the conventional guarantees that relate to criminal procedure such as transparency and the jurisdiction of the courts are ineffective from the point of view of data protection. Almost no consideration has been given to the possible negative effects of the proposed legislation for the social position of innocent citizens. For this reason, the Dutch DPA advised that a separate, robustly protected special regime be created for the handling of 'soft' information by the police.

#### **CounterTerrorism information point**

In 2005, the Dutch DPA analysed at the request of the Lower House the set-up of the *Contraterrorisme-Infobox* (CT Infobox) [Counter-Terrorism-Infobox]. The purpose of the CT Infobox is to ensure the practical implementation of existing statutory powers to exchange data regarding terrorism. An initial analysis by the Dutch DPA gave rise to a clarification by the Minister. More detailed analysis revealed that the involvement of the IND [Immigration and Naturalisation Service] contravenes the law. The boundary between intelligence activities and detection must be respected. It may be legitimate to cross that boundary, but there must be a clear demarcation that shows where intelligence work becomes detection work and the prosecution of criminal acts. In addition, effective supervision must be take place.

#### **Draft Sequestering of Data Powers Act**

On 1 January 2006, the *Wetsvoorstel bevoegdheden vorderen gegevens* [Draft Sequestering of Data Powers Act] entered into force, following a lead-in period of several years. The proposed legislation is based upon proposals from the *Commissie strafvorderlijke gegevensvergaring* [Collection of Information for Criminal Proceedings Committee]. The Act enables the judicial authorities and the Police to request data from social institutions and companies, if the data is required for detection purposes. At the beginning of 2005, the standing committee for Justice of the Upper House invited the Dutch DPA to a discussion within the framework of the preparation of the handling of the *Wetsvoorstel bevoegdheden vorderen gegevens*. The Dutch DPA made a case for two structural guarantees: the ability to test a demand in advance in the courts and systematic and regular checks regarding the processing of data in police records.

#### **Compulsory retention of telecommunications traffic data**

In 2005, the Dutch DPA strongly opposed the introduction of a general obligation to preserve what is known as telecommunications traffic data. Neither the usefulness nor the necessity for such a massive, preventative storage of telecommunications traffic data relating to 450 million European citizens had been demonstrated and no specific guarantees had been put in place. Both on a national and a European level, there was broadly-based political criticism with regard to the intention of the European Ministers

of Justice and the Interior to provide for compulsory storage of data in the form of a framework decision. This political opposition faded away during the course of the year.

### **Central Information Point for the Detection of Telecommunications**

Providers of mobile and landline telecommunications services – and, in the longer term, of internet access services are obliged to maintain a super telephone directory that can be consulted by the police, judicial authorities and intelligence services. The *Centraal Informatiepunt Opsporing Telecommunicatie (CIOT)* [Central Information Point for the Detection of Telecommunications] in Zoetermeer forms part of the Ministry of Justice and functions as an information hatch between the telephony sector and the authorities. Many telecoms providers also allow the CIOT to manage their database on their behalf. Following pressure from the Dutch DPA, a processing agreement was the subject of serious discussions during negotiations between telecommunications providers and CIOT. A judicial area agreement was also compiled. On a periodic basis, checks will be carried out in order to ascertain whether or not the data acquired by the Police and judicial authorities has been requested in a legitimate manner. Both agreements were ready to be signed in January 2006 by the Government and the telecom companies.

## **Combating fraud**

### **Blacklists**

Blacklists as a means of combating fraud and crime retained their popularity during 2005. In assessing the legitimacy of this type of list, the Dutch DPA places considerable emphasis upon whether or not the proposal submitted by the originating party provides sufficient guarantees that the data will be handled responsibly. These guarantees emerge from a consideration of the interests of the organisation and the entitlement of the individual to privacy.

In 2005, the *Kamers van Koophandel* [Chambers of Commerce] submitted a blacklist that was intended to detect fraud arising from the sale of advertisements, lotteries and unsolicited deliveries. The extent of fraud involving false invoices and of acquisition fraud proved to be sufficiently large as to cause the *Steunpunt Acquisitiefraude (SAF)* [Advertising Fraud Support Centre] to create a blacklist. SAF collects data and issues warnings relating to suspected acquisition fraud and of the senders of fraudulent invoices to organisations involved in detection and prosecution. The *Centraal Bureau Levensmiddelenhandel (CBL)* [Dutch Food Retail Association] wanted to maintain a blacklist concerning incidents in stores on behalf of its members. The purpose of this would be to prevent participating stores from becoming a victim of criminal acts that had been inflicted upon other members.

### **Linking of data to combat fraud**

Increased interest in benefit fraud at local authority level reflects the changed social climate associated with benefits and is directly linked to the financial interest of local authorities in establishing effective control of the implementation of the *Wet werk en bijstand* [Work and Social Assistance Act]. In the middle of 2005, the State Secretary informed local authorities of the ability to link data in order to combat fraud.

In order to do justice to the interest in the effective combating of fraud and the

interest in protecting the personal privacy of benefit recipients, the Dutch DPA submitted the memorandum entitled *Fraudebestrijding door bestandskoppeling* [Combating Fraud by linking of data] to the State Secretary for Social Affairs in the middle of 2005.

In many instances, control that is exercised by linking and granting access to data means that personal data is used for a purpose that is different to the one for which the individual to which they relate believed they were to be used. The Dutch DPA feels that the liberal linking of data containing details of large groups of unsuspected citizens is out of proportion and undesirable. The basic principle underlying the combating of fraud by linking and granting access to data must be that the ability to carry out checks upon an individual benefit recipient can only be increased according as there is a stronger suspicion of fraud. This method is comparable to the one in use at the *Belastingdienst* [Netherlands Tax and Customs Administration].

In December 2005, the State Secretary informed the Lower House of the Dutch Parliament of the electronic access to a number of databases that had been granted to local authorities. On that occasion, the State Secretary referred to the Dutch DPA's view of linking and granting access to data as a "clear framework for decision-making" for local authorities.

## Information infrastructure

The Government's information infrastructure is undergoing a major overhaul that will be completed during the next two years. The worrying thing is that there is a lack of an overarching vision with regard to policy concerning personal information. As a result, a debate in Parliament about the overall policy on personal information has yet to take place.

### Citizens Service Number

In 2005, a draft law containing general stipulations for the *burgerservicenummer* (BSN) [Citizens Service Number] was submitted to the Lower House. The draft law introduces the use by the Government of the BSN as a general personal identification number. The draft law contains stipulations governing the generating, distribution, issuing and management of the numbers. It does not however provide an arrangement that will promote the careful use of the BSN in practice. The Dutch DPA already pointed this out in its recommendations relating to the draft law that were issued in 2004.

In view of the fact that in the opinion of the Dutch DPA, the draft law did not take sufficient account of its objections, the Dutch DPA expressed its concerns in this regard to the Lower House in October 2005. The Dutch DPA issued a warning to the effect that the draft law containing general stipulations for the implementation and the use of the BSN contains serious shortcomings with regard to the limitation of risks associated with the introduction and use of such a number. The political parties in the Lower House asked the Minister questions with regard to the points raised by the Dutch DPA.

The Dutch DPA regards it as a matter of considerable importance to citizens, the protection of their personal data and the social acceptability of the introduction of the BSN that clear regulations be laid down in the form of legislation concerning: a) the circumstances in which use of the BSN is permitted; b) which government bodies (and possibly companies) are permitted to make use of the BSN; c) an obligation to notify individuals of any errors that may be discovered; d) the availability to individuals of

## Objectives for 2006

IN 2006 THE FOLLOWING ISSUES AND OBJECTIVES WILL BE PRIORITISED:

- **Health insurers throughout Europe inspected**

In 2005, the Dutch DPA was one of the instigators of the implementation of a joint enforcement initiative by all EU data protection authorities. In 2006, harmonised enforcement inspections will be carried out on health insurers. The results of the inspections will be compiled and published in a joint report.

- **Information security in hospitals**

In 2005 there was much publicity surrounding information security in hospitals. In 2003, the *Inspectie voor de Gezondheidszorg (IGZ)* [Healthcare Inspectorate] carried out a study entitled 'ICT in hospitals'. In continuation of this study, the Dutch DPA and the IGZ will carry out a joint study in 2006 into information security in hospitals.

- **Electronic Child File**

The intention is to introduce the electronic child file into child healthcare with effect from 1 January 2007. The development of a child and the distinguishing features of the child's environment will be recorded in this file commencing from (before) birth. The child file will be linked to the future *burgerservicenummer* [Citizens Service Number]. In 2006, the Dutch DPA will focus intensively on this development and provide advice where necessary.

- **Intervention teams for combating fraud**

There is a network of regional intervention teams operating covering the Netherlands with the aim of tackling the black economy, illegal employment, benefit fraud and tax fraud. Municipalities, the *Belastingdienst* [Tax and Customs Administration], the *Sociale Verzekeringsbank* [Social Insurance Bank], the *Arbeidsinspectie* [Health and Safety Inspectorate], the *Uitvoeringsinstituut Werknemersverzekeringen* [Employee Insurance Schemes Implementing Body] and the Public Prosecution Service work together in these teams. In 2006, the Dutch DPA will conduct a study into compliance with the duty to provide information as well as into the legitimacy of sharing information and the use of police information by intervention teams.

- **Combating benefit fraud**

A number of proposals have been made to combat benefit fraud which all to a greater or lesser degree infringe upon the personal privacy of benefit recipients. Municipalities are requesting access to more and more files from different organisations. In 2006, the Dutch DPA will organise a meeting of experts to discuss a clearer system for combating this type of fraud. Benefit recipients must not be regarded as any more suspicious than any other citizens. Research into compliance by the Social Security Fraud Department with the duty to provide information will also be carried out in 2006.

- **Administrative burden and privacy: Binding Corporate Rules**

In 2006, the Dutch DPA will process and co-ordinate permit applications from a number of large multinationals according to the new uniform procedure for applying for a permit to transfer personal data to countries outside the European Union and for the co-ordinated European processing thereof.

- **The obligation to inform citizens**

At the end of 2005, TNS/NIPO carried out a study within five sectors into compliance with the duty to provide information in accordance with the *WBP* [Dutch Data Protection Act] and compliance with the duty to provide information as experienced by citizens. The results will be published at the beginning of 2006. In 2006, the study will lead to initiatives in the different sectors aimed at raising awareness of and compliance with the duty to provide information.

- **Internet publications and privacy**

The internet raises questions among users about their privacy and the security of their personal data. The internet leaves the Dutch DPA open to questions about its competence as a supervisory authority and the possibility of effective supervision on the internet. In 2006, the Dutch DPA will organise a symposium on this subject and will also publish a first exploratory position paper and a number of information sheets.

- **RFID and privacy**

Radio Frequency Identification is a technology whereby all manner of objects can be fitted with small, readable tags (minuscule radio chips). The data that the chip gives about the object and what the person requesting the information can and may subsequently do with these data also concerns the protection of personal data. In 2006, a public consultation will be held on this matter and an external report generated on the basis of this consultation.

- **Biometrics in travel documents**

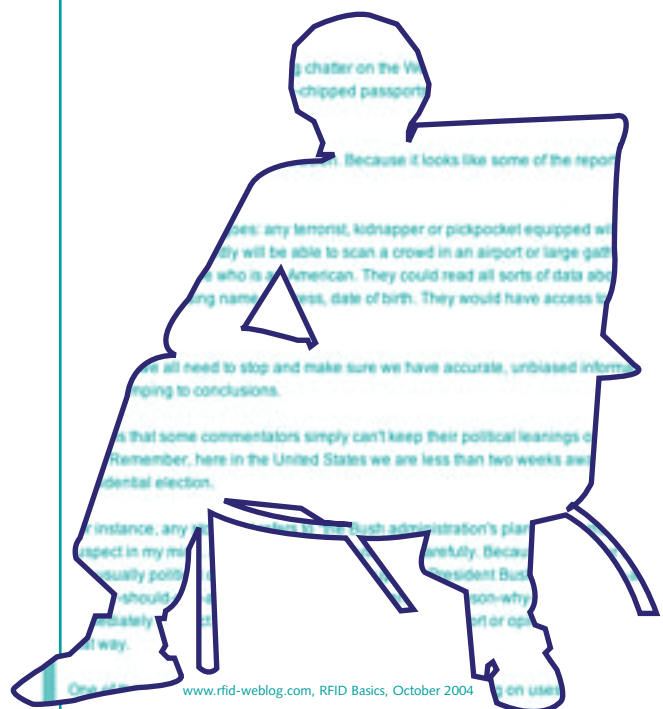
An increase in the use of biometrics in travel documents is anticipated in 2006. The Dutch DPA will organise a meeting of experts to discuss the value of, the need for and the possible drawbacks of large-scale, centralised storage of biometric data.

- **Citizens Service Number**

The introduction of the *burgerservicenummer* [Citizens Service Number] and the use of this number in the healthcare sector has been postponed. Further to its letters to the Lower House of October 2005 and January 2006 on this matter, the Dutch PDA will continue to advise the Ministers and/or Houses where necessary.

- **Security and privacy**

In collaboration with the Minister of the Interior and the Minister of Justice, the Dutch DPA has asked Professors H.R.B.M. Kummeling and E.R. Muller to carry out research to find a good balance between 'security' and 'privacy'. The Dutch DPA will organise a conference on this subject in 2006.



the services of an ombudsman and e) the requirements with regard to the data security measures to be applied to the databases that make use of the BSN.

### **Streamlining of the use of fundamental data**

As part of the streamlining of the use of basic data that was re-launched in the middle of 2004, the development of six fundamental databases (individuals, buildings, addresses, topography, land register and companies) is envisaged. In addition, there is also an intention to designate policy administration (the administration of employee's insurance policies), the vehicle registration system and the income database at the *Belastingdienst* [Tax and Customs Administration] as fundamental databases. It will become compulsory for the Government to make use of data contained within these databases and it will no longer be permissible for such data to be requested from individuals or from companies. This equates to the principle of one-off provision of data and compulsory re-use of data. The introduction of the BSN and the associated system is closely related to this.

In 2005, the Dutch DPA issued recommendations regarding three draft laws that form part of this programme. These were the *Wetsvoorstel register van ondernemingen en instellingen* [draft law governing a register of companies and institutions (to replace the current *Handelsregisterwet* [Commercial Register Act]), the *Wetsvoorstel basisregistratie kadaster en geografie* [draft law governing the fundamental database for land registration and geography] and an amendment to the *Wet gemeentelijk basisadministratie persoonsgegevens* [Municipal Register Act]. These draft laws stipulated the compulsory use by government bodies of specific data. These closely followed the rules contained in the current legislation.

### **Information handling by the Police**

The current *Wet politieregisters* [Police Files Act] is undergoing a fundamental revision. In 2004, the Dutch DPA issued recommendations to the Minister of Justice as to the draft *Wet politiegegevens* [Police Data Act]. The Dutch DPA agreed with the structure for the processing of police files within the police force, but criticised certain sections of the proposed law.

At the end of 2005, the Dutch DPA informed the standing committee for Justice of the Lower House of its criticisms of the final draft law, due to the fact that essential points contained in its recommendations had not been followed: a) data are not assigned a code that indicates the reliability (the difference between soft and hard information) and the inherent risks, b) insufficient guarantees have been included against the data being divulged to third parties that are of minimal reliability, c) no additional guarantees have been created for data relating to unsuspected persons and d) the law enables an overly extensive gathering of data relating to unsuspected persons. In addition, it is also necessary to stipulate, in the form of legislation, the compulsory auditing of the information management systems within the Police, such provisions to include an obligation to carry out self-evaluation.

### **Schengen Information System II**

In 2005, the Dutch DPA acted as Chair of the Joint Supervisory Authority [JSA] of the Schengen system. The most significant development remained the development of the Schengen Information System (SIS) II. The existing Schengen Information System is insufficient for the expansion to include the new member states and is not equipped to hold biometric data.

In accordance with the 2004 recommendations relating to SIS II, the JSA Schengen issued recommendations in October 2005 in relation to the legal framework for the new information system, as put forward by the European Commission. The JSA Schengen also has a number of fundamental objections to the legal basis being proposed. It is not clear which European legal frameworks shall apply in the case of SIS II and who will be responsible for it. The purpose of data processing is insufficiently well defined, as a result of which the legal basis does not comply with the basic principles of data protection. In addition, the draft contains insufficient provisions for the supervision exercised by national and European supervisory authorities. The role of the European Commission, the European Data Protection Supervisor (EDPS) and the national data protection authorities, remain unclear within the draft law. All of the current tasks of the JSA need to be reinserted into the new supervisory structure.

### **European visa information system**

In 2005, the Article 29 Working Party issued an opinion regarding the proposed introduction of a European visa information system (VIS) that would enable visa information to be exchanged between member states that have abolished internal border controls. No single European system is currently comparable with the VIS, in terms of its scope or capacity. Personal data, including biometric data, of millions of people will be stored in a central database and will be exchanged between member states. The proposal provides for extensive access to the VIS for a broad range of purposes.

For this reason, the working party recommended that the purpose for which data are processed within the VIS be precisely defined and limited to what is strictly necessary in order to improve common visa management. Systematic access must be limited to the authorities responsible for implementing visa policy. We must not lose sight of the purpose for which the various European systems have been developed. The drive to improve the interoperability between European databases such as the VIS, SIS II and Eurodac must not give rise to a situation in which authorities actually have access to data that they are not permitted to use.

## **Investigation and supervision**

The compliance, by governments, companies and other organisations, with the obligation to provide information gained particular attention during 2005. Awareness-raising in this regard has been enhanced and a number of studies carried out into compliance with the duty to provide information that is to be published in 2006. The duty to provide information is an essential precondition for individuals, in order to be able to view and correct the information, so as to preserve their own interests. At the request of the Dutch DPA, TNS-NIPO Consult carried out a survey into the obligation to provide information within three sectors: doctors' surgeries, educational institutions and housing associations. In addition, a representative sample of individuals were questioned as to their opinions of the value of the obligation to provide information and their experiences with regard to the manner in which data controllers inform them about how their personal data will be used. It immediately became apparent that there were shortcomings in the manner in which their data is handled.

### **Private detective agencies**

In 2005, two studies were carried out by private detective agencies. In evaluating compliance with the WBP [Dutch Data Protection Act], the *Privacygedragscode voor particuliere onderzoeksbureaus* [Privacy code of conduct for private detective agencies] was applied, which took effect on 13 January 2004. With effect from 1 June 2004, the Minister of Justice made compliance with that code of conduct compulsory for all private detective agencies, as a condition for the awarding of their licence. The study for Dutch DPA was the first that was carried out since the sector had been regulated.

One of the studies related to compliance with the duty to provide information. For this purpose, a random sample consisting of thirty agencies were approached, as part of an enquiry in order to ascertain the extent and nature of compliance with the laws governing the provision of data. The second study consisted of in-depth, on-site studies carried out on site at approximately three detective agencies. In addition to compliance with the duty to provide information, this study also tested various other aspects of the WBP, such as compliance with the storage limit of data. The results of this will be cleared up in 2006.

### **Investigation at healthcare insurance companies**

In spring 2005, the Dutch DPA carried out a study at the premises of three healthcare insurers. The purpose was to get a better picture of the types of processing of personal data that takes place within healthcare insurance companies, as well as of any potential problems. The study was also carried out with a view to evaluating the *Addendum Zorgverzekeraars* [Healthcare Insurers' Addendum to the Code of Conduct].

The purpose of the European working programme to improve the implementation of the Privacy Directive was, amongst other things, to reinforce its use. In 2005, the Article 29 Working Party decided that the first joint study of national data protection authorities shall focus upon healthcare insurers. The purpose of the study is to ascertain whether and in what manner the various countries comply with the privacy rules in this particular sector. The study is scheduled to commence in 2006.

### **Investigations at reintegration companies**

Dutch DPA carried out an exploratory investigation into the practical implementation of the reintegration of benefit recipients and sick employees. The reports of the studies were submitted on 12 December 2005 to Borea, the *Brancheorganisatie Reïntegratiebedrijven* [Sector Organization for Reintegration Companies].

The conclusion of the study into the reintegration of benefit recipients was that the manner in which reintegration companies process personal data is to a large extent determined by the customers, i.e. the local authorities. As customers, local authorities seem to require more information in reports about benefit claimants than is actually necessary.

The study into reintegration of employees suffering ill-health confirmed the expectation that in practice, reintegration companies are experiencing difficulties, due to a loophole in the labour legislation. The legal basis, as it currently exists, is insufficient when it comes to reporting about the possibilities for the resumption of work and the extent to which sick employees lend their support. Under the regulations as they currently exist, reintegration companies are not permitted to report medical information to the employer or occupational health and safety service.

### **Study into the destruction of tapped lawyer-client conversations**

In 2005, a study was carried out into compliance with the regulations for the destruction of tapped telephone conversations between lawyers and their clients. Based on the stipulations contained in the *Wetboek van Strafrecht* [Penal Code], those conversations, which are subject to the professional confidentiality of lawyers, must be destroyed. The Dutch DPA carried out spot checks in order to ascertain whether or not such conversations ought to have been destroyed, were in fact destroyed. That study will be completed and published in 2006.

### **Investigations at Europol**

In 2005, the Dutch DPA examined the processing of personal data by the Dutch Desk at Europol. Europol is the European police service for the combating of cross-border severe, organised crime. Each of the member states that are signatories to the Europol Agreement possesses a national contact point for the exchange of information with Europol and the other member states. The Dutch department, known as the Dutch Desk, forms part of the *Korps Landelijke Politiediensten (KLPD)* [National Police Services Agency]. The study revealed that a positive image was forthcoming with regard to the manner in which data processing takes place.

In 2005, the Dutch DPA also took part in the annual audit of Europol's systems by the Joint Supervisory Body of Europol (Europol JSB). The annual checks carried out reveal again and again the great importance that is attached to the reasonable quality of the data supplied by the member states. The 2005 audit also examined the newly-developed Information System at Europol.

### **Exchange of police data with the Netherlands Antilles**

The rapid and careful exchange of police data between the Netherlands Antilles and the Netherlands plays an important role when it comes to combating crime. In order to enable such an exchange of data to take place, the Ministers of Justice, Foreign Affairs and Kingdom Relations and the Minister of Justice of the Netherlands Antilles compiled and signed the *Protocol gegevensuitwisseling tussen de Nederlandse Antillen en Nederland* [Protocol for the exchange of data between the Netherlands and the Netherlands Antilles]. The Dutch DPA exercises supervision over the exchange of data from the Netherlands to the Antilles and with regard to the system that was used. At the time, an agreement was made between the ministers involved that the Dutch DPA would determine the state of affairs regarding the exchange of data and whether or not the protocol is being adhered to. This study took place in the autumn of 2005 and is scheduled for publication in 2006.