Review of 2002

Security was the primary focus of political and public debate in 2002. Amid the general calls for greater decisiveness, supervision and control, various prominent administrators and politicians made a caricature of privacy. Privacy protection was portrayed as an impediment to public safety; privacy legislation therefore required reform. In November, the administration proposed that everyone over the age of twelve should have a legal obligation to identify themselves. It was also suggested that, with a view to aiding the fight against crime and terrorism, all telecommunication traffic data should be retained for an extended period. The Dutch Data Protection Authority (DPA) is very concerned that a simplistic introduction of greater police powers could seriously undermine the rights and interests of ordinary citizens.

Furthermore, the Dutch DPA strongly refutes the notion that privacy protection acts as a barrier to the resolution of social problems by hindering cooperation between various authorities. It is the Dutch DPA's conviction, borne out by experience, that privacy protection is one of the success factors for effective government.

There are very few legitimate government objectives whose realisation may be impeded by privacy rules. Provided, that is, that such rules are taken into account from the outset in the design of organisational structures, information systems and procedures and the formulation of policy.

Privacy and security

The citizen's interest in privacy must always be weighed up against other important interests. International treaty law, European directives and our own country's constitution and privacy legislation define the parameters within which this should take place. These parameters form part of the framework of ground rules on a government's behaviour towards its citizens. Privacy rules require that careful consideration is given to the object, effectiveness and proportionality of government action and that sufficient safeguards exist against the abuse of power. To set privacy legislation aside is to accept that such controls and safeguards are not required.

Lack of respect for the privacy of the individual ultimately erodes public faith in government. Citizens who have nothing to hide deserve a government that consistently takes privacy protection into account when formulating policy, designing information systems or defining the responsibilities of the individual.

Hence, the right to privacy is fundamental to the security that a democratic constitutional state affords its citizens. Removal of the right to privacy denies the honest citizen an important safeguard and undermines democracy itself.

Compulsory identification

In December 2002, legislation was proposed, providing for the introduction of compulsory identification. Early in 2003, the Dutch DPA advised against bringing a bill before parliament. The proposed legislation fails to strike an appropriate balance between the rights and obligations of the individual and those of the government.
A permanent obligation would be placed upon the citizen without any evidence that specific obligations are not sufficient. Criminalising failure to identify oneself would create a situation in which any member of the public was liable to be regarded as a suspect.

The question of whether a limited or general obligation to identify oneself should be introduced has been debated in the Netherlands for the last twenty years. Hitherto, it has always been concluded that a general requirement would be unduly onerous. Given that the current proposal is not based on fresh arguments in this regard, its implementation would constitute a contravention of the European Convention on Human Rights, which requires that any infringement of individual privacy must be adequately justified.

Camera surveillance of public places

Public camera surveillance remains a topical issue and is in need of better statutory regulation. Such surveillance has become generally accepted as a legitimate means of furthering security and public order, although initial evaluations of CCTV projects suggest that the security benefits are not as great as has sometimes been suggested. During the course of 2002, the Dutch DPA published two advisory reports regarding the Camera Surveillance of Public Places Bill. In the interests of legal clarity, a statutory framework is important. The Dutch DPA fully supported the proposal that the authority to install cameras should be given to mayors by order in council. Such authority is consistent with a mayor's responsibility to maintain public order.

The proposed legislation would permit the installation of CCTV in churches and comparable locations. Is it the intention that the government should have the power to place surveillance cameras in churches, mosques and other places of worship in the name of public order?

Electronic government

The government's management of information is gradually becoming more structured, as the authorities seek to operate as efficiently and reliably as possible. This development brings significant threats to and opportunities for the protection of personal information. In 2002, the Dutch DPA set out its vision in a study report entitled *Elektronische overheid en privacy: bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid* (Electronic government and privacy: the protection of personal data in the government's information infrastructure). Intended primarily for policy-makers, the report discusses privacy-design principles for information systems and analyses the scope allowed by the privacy rules.

Trust is a vital precondition for a functional information infrastructure. The Dutch DPA therefore has reservations about the plea for every citizen to have control over his or her personal data. The government should undoubtedly ensure optimal transparency, but there are practical limits on the scope for informational self-determination. The Personal Data Protection Act deliberately provides for a system of checks and balances, in which consent and objection merely play a corrective role. What is more important is that the government should of its own accord operate in a transparent manner that promotes trust.

Results secured in 2002

In last year's annual report, it was announced that in 2002 priority would be given to securing the following results:

- **Electronic government**
  In its study report *Elektronische overheid en privacy* (Electronic government and privacy), the Dutch DPA set out how government can use ICT to work more efficiently and effectively, while preserving or enhancing privacy safeguards. This vision has contributed to the government's policy on the streamlining of population records and the use of personal ID numbers.

- **ICT in healthcare**
  In its study report *Privacy bij ICT in de zorg* (Privacy and the use of ICT in the healthcare sector), the Dutch DPA indicated how privacy protection can be more effectively institutionalised in the healthcare sector. The report's recommendations have been widely publicised within the sector. Taking proper account of privacy issues at an early stage is a critical success factor in the context of new developments in this field.

- **Research and statistics**
  The policy document *Privacy bij wetenschappelijk onderzoek en statistiek* (Privacy in the context of scientific research and statistics) clarifies the legal rules governing the use of personal data in this field. The document also provides a framework for the development of a code of conduct to serve as guidance on compliance with the rules in practical situations. The Royal Dutch Academy of Science has taken the initiative in this regard.

- **Employees**
  An updated version of *Goed werken in netwerken* (Working well in networks), a new *Raamregeling voor het gebruik van e-mail en internet* (Framework for the use of e-mail and the Internet) and a brochure entitled *Privacy: checklist voor de ondernemingsraad* (Privacy: checklist for the works council) were published, emphasising the importance of proper privacy protection at work. In addition, the groundwork was done for the publication of a document on the position of workers who have fallen ill.

- **Trade information**
  It did not prove possible in 2002 to achieve consensus within the trade information sector regarding clear guidelines on the lawful processing of personal data or a mechanism for ensuring compliance with such guidelines. This was in spite of the fact that the need for standards and safeguards was emphasised by the findings of Dutch DPA investigations. Given this situation, the Dutch DPA has decided to take firmer action.

- **Telecommunications use**
  The Dutch DPA has conducted exploratory research into the processing of data on the use of telecommunications. The findings served as a basis for a workshop organised in September 2002 in conjunction with the Institute for Information Law and supported by the Netherlands OPTA (*Onafhankelijke Post en Telecommunicatie Autoriteit*, Independent Post and Telecommunications Authority). The research findings were recorded in a publication entitled *Verkeersgegevens* (Traffic Data), which will also be used as a basis for further activities in this field.

Public service numbers

Using its vision of electronic government as a starting point, the Dutch DPA contributed to the report produced by the interdepartmental Van Thijn Committee, entitled *Persoonsnummerbeleid in het kader van identiteitsmanagement* (Personal ID number policy in the context of identity management). The Dutch DPA was represented on the committee. The administration accepted the report's recommendations and announced its intention to put forward proposals for a 'public service number' in 2003.

The introduction of a public service number system would facilitate the clear association of data with the individual citizen and thus support efficient client-oriented government. The use of a number would enable the linkage of data held by different authorities and would therefore help in the detection and prevention of (identity) fraud.

The planned sector-based control of personal ID numbers is consistent with the Dutch DPA's vision of electronic government and its preference for sector and chain numbers. Under the proposals, for example, the justice sector and the healthcare sector would each have their own number systems. Furthermore, the lawful processing of data will be facilitated by the trust functions, which include Privacy-Enhancing Technologies, i.e. technical measures built into the information systems to safeguard privacy.

- **Special police records**
  An improvement was discernible during 2002 in the protection of privacy in connection with the records of 'criminal investigations' by the police. More attention is now being given to both the control and the structural supervision of such records by most forces. Agreement was also reached regarding the streamlining of the procedure for dealing with requests for the disclosure of information by people to whom such records relate. The conclusions were widely publicised within police circles and the public prosecution service.

- **Public register of notifications**
  The Dutch DPA website now provides public access to a register of personal data processing activities notified to the authority. An improved version of the software for submitting notifications on diskette has been released and Internet notifying is now possible. The number of notifications received rose sharply in the course of 2002. The register of data protection officers can also now be consulted via the Dutch DPA's website.

- **Prior checks**
  The number of prior checks into personal data processing activities involving special risks (articles 31 and 32 of the Dutch Personal Data Protection Act) rose markedly in 2002. An overview of these investigations will be posted on the Dutch DPA's website in the course of 2003. In conjunction with the relevant stakeholders (social security investigation teams, municipal social services departments, etc), standards have now been developed covering various common processing activities.

- **Enforcement plan**
  In 2002, an Intervention, Complaints and Appeals Department was set up. The development of an enforcement plan has since led to the creation of a number of tools that enable the Dutch DPA to make effective use of its new powers. The first steps have also been taken towards the systematic checking of compliance with the obligation to notify personal data processing activities.

Social security files

Operation of the social security system requires extensive checks to be made on individual clients. In February 2002, a file investigation was carried out at three social security offices. This involved inspecting client files to establish whether the information held was actually necessary for the assessment of individual clients' entitlement to benefit (i.e. whether the necessity principle was being complied with). In addition, steps were taken to establish where the social security offices obtained information and with whom they shared information. The Dutch DPA formed a positive impression of the way the three offices handled personal data, but is considering making supervisory visits to social security offices in the future.

New social security legislation

At the end of 2002, the Dutch DPA published its response to the proposed new social security legislation, since dubbed the Work and Income Bill. The new legislation is to replace a variety of existing laws and regulations. By giving municipal authorities greater freedom in the definition of individual rights and obligations and in the provision of services, the administration hopes to promote the reintegration of people seeking employment.

The Dutch DPA had previously asked the Minister of Social Affairs and Employment on a number of occasions to draw up clear rules on the sharing of personal data in the context of reintegration. However, the bill does not indicate how in practice data should be processed in connection with reintegration. It appears that a great deal has been left to the discretion of individual municipalities. There is consequently a danger that differences will arise between municipalities in terms of the way reintegration activities are organised.

Social security investigation and fraud teams

Efforts to combat social security fraud received a lot of attention in 2002. A variety of organisations are involved in the investigation of such fraud: (municipal) social security investigation teams, *Regionale Interdisciplinaire Fraudeteams* (Regional Interdisciplinary Fraud (RIF) teams) and the Sociale Inlichtingen- en Opsporingsdienst (Social Security Investigation and Detection Service, SIOD). Having been notified of certain data processing operations, the Dutch DPA carried out a prior check to assess whether the activities were organised on a lawful basis. Similar checks were initiated into the investigative activities of the Uitvoeringsinstituut Werknemersverzekeringen (Employee Insurance Scheme Executive Body) and the Sociale Verzekeringsbank (Social Insurance Bank).

The Dutch DPA assessed the process definition for covert observation drawn up by one of the RIF teams, as well as the associated working practices. In principle, the process definition was considered to provide adequate safeguards for the lawful processing of personal data. It was agreed that the process definition would be made available to other RIF teams by way of example. A similar approach was taken by the Dutch DPA in relation to municipal social security investigation teams.

It is hoped that the strategy adopted can lead to general nationwide harmonisation of the covert observation practices used by RIF teams and (municipal) social security investigation teams. This will be beneficial in terms of legal clarity and compliance with the Personal Data Protection Act, while also simplifying the necessary notification of data processing activities.

Blacklists

Crime-prevention was also very much on the agenda of the business community in 2002. Dissatisfied with the protection offered by the police and judiciary, businesses sought their own means of combating misconduct and fraud by customers and personnel. Among the tools adopted was the blacklist. Against this background, one of the Dutch DPA's focuses during 2002 was the maintenance of a shared blacklist by the financial services industry.

It is undeniable that a business may have a legitimate interest in operating a blacklist. However, it is important to consider whether the significance of that interest is sufficient to justify the consequences of inclusion for the blacklisted individual. If a business decides to introduce a blacklist, steps must be taken to ensure that the system is operated fairly. Without proper safeguards, a blacklist is unlawful.

The use of warning lists to address employee fraud attracted considerable publicity. The Dutch DPA examined a number of lists. The consequences of blacklisting depend to a considerable extent on the scope of the blacklist. Such a list may be used purely in connection with sensitive functions, or for all appointments; it may be used only within a particular business or chain, or it may be shared by an affiliated group of companies or throughout a particular industry. The wider the scope of the list, the stricter the inclusion criteria must be.

Working well in networks

Careful justification and organisation of checks can ensure that necessary fraud prevention measures do not undermine the relationship between employer and employee. The key is achieving an appropriate balance between the interests at stake. Responsible supervision of the (private) use of e-mail and the Internet at work requires a privacy test and good workforce consultation or the cooperation of the works council. With a view to promoting equable measures within employment organisations, in 2002 the Dutch DPA published an updated version of *Goed werken in netwerken* (Working well in networks), a new *Raamregeling voor het gebruik van e-mail en internet* (Framework for the use of e-mail and the Internet) and a brochure entitled *Privacy: checklist voor de ondernemingsraad* (Privacy: checklist for the works council). All these publications attracted a great deal of attention in 2002.

Privacy and the use of ICT in the healthcare sector

In 2002, the Dutch DPA also published a study report entitled *Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg* (Privacy and the use of ICT in the healthcare sector. Data protection in healthcare information infrastructures). The report was intended as an overview of the privacy issues associated with the use of ICT in the care sector. The numerous proposed policies, experiments and trends relating to the use of ICT in healthcare will lead to the formation of an electronic identity infrastructure, an electronic information infrastructure and changes in the organisation and funding of healthcare. Most of today's ICT applications have not been designed with sufficient thought for privacy. Within the healthcare sector, success depends to a significant extent on taking proper account of privacy at an early stage.

Healthcare reforms are aiming at greater competition amongst care providers and amongst health insurers. The amount paid for care must be related to the actual costs.

In the context of these reforms, the so-called Diagnose-Behandeling Combinatie (Diagnosis-Treatment Combination, DTC) system is to be adopted. It is important that the government ensures that this system's design takes account of the different roles played by health insurers and the other parties involved in healthcare. Detailed treatment information should not be disclosed without careful consideration. The privacy laws and the principle of medical confidentiality impose strict limitations on the processing of (certain forms of) personal data.

Trade information agencies

A thoroughly unsatisfactory situation exists in the trade information agencies sector. The Dutch DPA had to perform another major investigation at such an agency in 2002. Clearly something more than incidental checks are required to bring this industry into line with the law on the processing of personal data. The business community has a self-evident interest in good credit rating and debt-recovery information. However, a balance has to be found between this interest and society's general interest in the reliable and fair use of personal data by the authorities and by the business community. The best solution is likely to lie in further regulations on the way personal data are obtained for credit rating and debt collection purposes.

Telecommunications

The telecommunications sector has to contend with a variety of regulatory controls in the form of European directives, national legislation and jurisprudence. The Dutch DPA realises that uncertainty exists within the sector regarding the application of privacy standards. In 2003, the Dutch DPA accordingly intends to provide telecommunications companies with practical advice regarding such matters. In conjunction with the Netherlands Independent Post and Telecommunications Authority (OPTA), the Dutch DPA has initiated investigations into the sale by KPN Telecom of address data linked to so-called 'ex-directory' numbers for marketing purposes. The Dutch DPA hopes to extend its cooperation with the OPTA on supervisory issues.

The privacy issue that exercised the industry most in 2002, was the retention and use of traffic data. Telecom service providers gather huge volumes of data on the activities of private individuals (use of landlines, mobile phones and the Internet). Such data are retained after the communication activities cease and can be of great commercial value to providers in the context of a wide variety of innovative services. Telecommunications data are strategically valuable for marketing purposes. In 2002, the Dutch DPA undertook an exploratory study into charging and settlement within the telecommunications industry and made preparations for an investigation into the actual use of traffic data.

Investigation and traffic data

With support from the Dutch DPA, the Institute for Information Law at the University of Amsterdam organised a seminar in September 2002 concerning the technical, criminal and public-law issues surrounding traffic data. At the seminar, the Dutch DPA again called for a cautious approach to the retention of traffic data. Taken in context, traffic data can be highly informative. Hence, the constitutional provisions regarding confidential communication are of relevance in relation to its use.

In the post-September 11 climate, strong political support developed for the prolonged retention of such data for use by investigative agencies. At the European level, inter-governmental discussions were held in 2002 regarding the possibility of compulsory systematic retention of all telephone, fax, e-mail and Internet traffic data. The suggestion was that such data would have to be made available to the police, the Public Prosecutor and the security services. Such a move would be a serious threat to the privacy of the individual.

On 3 September 2002, the Dutch DPA informed the Minister of Justice that it would consider a general obligation to retain traffic data for a year or more to be disproportionate and wholly unacceptable. A joint statement to similar effect was issued on 11 September 2002 by Europe's data protection authorities, meeting at the time in Cardiff. European regulations allow traffic data to be retained for law-enforcement purposes only for a limited period and insofar as retention may be considered necessary, appropriate and proportional in a democratic society.

Privacy-Enhancing Technologies

In recent years, the Dutch DPA has invested substantially in developing and propagating the concept of Privacy-Enhancing Technologies (PET). At the PET symposium organised by the Dutch DPA in May 2002, the message was that PET had proven its worth in practice. Meanwhile, PET has been accorded a significant role in the government's planned personal ID number policy.

The aim of the symposium was to demonstrate the practical benefits of PET to policy-makers in the public and private sectors. By designing information systems to take account of privacy rules, it is possible to ensure – or at least go a significant way towards ensuring – that personal data are processed in a lawful way. In other words, one can achieve privacy by design. A situation in which privacy-compromising action is impossible is preferable to a situation where such action is prohibited. Symposium participants were told about three PET-protected information systems already in use in the Netherlands' healthcare sector, and about application of the PET concept in Canada and Germany.

Certification

The Personal Data Protection Act assurance products *WBP Zelfevaluatie* (Personal Data Protection Act Self-Evaluation) and *Raamwerk Privacy Audit (Privacy Audit Framework)* proved popular in 2001 and 2002, as did the Dutch DPA study report *Beveiliging van persoonsgegevens* (The protection of personal data) (2001). However, the Dutch DPA put less emphasis on publicising this approach in 2002, focusing primarily on privacy certification instead. In this context, the object has been to provide commercial audit organisations with a framework for privacy certification. In close consultation with those representative organisations that act as accreditation bodies, a scheme has been developed for the accreditation of privacy auditors. Certification criteria have been formulated using the *Privacy Audit Framework* as a primary reference. A preliminary structure has been developed for a certification scheme and a number of representative organisations have agreed to act as accreditation bodies, so that auditors may be accredited to issue privacy certificates for particular processing activities.

Targets for 2003

The main targets that the Dutch DPA will pursue in 2003 are as follows:

- **Advice on legislative proposals**
  Article 51, paragraph 2, of the Personal Data Protection Act states that the Dutch DPA has to be consulted about any proposed legislation or general administrative regulations which relates exclusively or to a significant extent to the processing of personal data. In consultation with the relevant government departments, the Dutch DPA will develop parameters to ensure that this statutory requirement is complied with.

- **Data protection officers**
  In accordance with articles 62 to 64 of the Personal Data Protection Act, more than a hundred data protection officers have now been registered with the Dutch DPA. Contact with this growing body of internal supervisors will be consolidated by the Dutch DPA so that there is effective practical interaction between the authority and the individuals concerned.

- **Camera surveillance**
  A growing number of municipalities have been installing camera surveillance systems in public places. The Dutch DPA will investigate how this supervision operates in practice and how privacy issues have been taken into account by the municipalities concerned.

- **Sickness leave**
  Changes to the social security system and in society at large have affected the position of an employee before, during and following a period of sick leave. The Dutch DPA will publish a study report dealing with the privacy issues surrounding the position of employees who take sick leave and with other relevant developments.

- **Police records**
  Following on from the Dutch DPA's earlier activities in connection with the records kept by Criminele inlichtingeneenheden (Criminal Investigation Units, CIEs), checks will be performed at the offices of a number of these units. These checks will draw partly upon the findings of the CIEs' internal evaluations.

- **Telecommunications**
  In practice, the provision of telecommunications services raises a number of privacy-related issues. In collaboration with the OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit, Independent Post and Telecommunications Authority), the Dutch DPA will develop information material to assist service providers. The Dutch DPA will also focus on the obligation to notify data processing activities and on prior checks in the telecoms industry.

- **Certification**
  Output from the earlier Audit Approach Project forms a basis for the development of a system of privacy certification. In conjunction with organisations interested in acting as accreditation bodies, the Dutch DPA will develop this system further and prepare for its implementation. In doing so, the authority hopes to promote compliance with privacy legislation by self-regulation.

- **Website**
  A well-designed website is a central element of the Dutch DPA's communication strategy. The accessibility of the Dutch DPA's website will be improved by, for example, the use of theme files and the creation of a separate section for data subjects' frequently asked questions. The site will also give details of the Dutch DPA's policy in relation to its various tasks.

- **Notification obligation**
  The obligation to notify the Dutch DPA regarding personal data processing activities is important in relation to transparency and accountability. With a view to enforcing compliance with the obligation, systematic checks will be performed. In addition, the authority will make use of its power to impose administrative penalties in the event of non-compliance.

- **Staffing plan**
  In order to ensure the authority's ability to discharge its new responsibilities in the field of supervision and enforcement, the Dutch DPA's structure and staffing arrangements will be reviewed. In the course of the year, a new staffing plan will be drawn up, incorporating new or modified job profiles.