Review of 2001

More than anything else, the digital revolution influences the way society handles information, including personal data. Citizens and consumers welcome the benefits of digital service provision with open arms. But, at the same time, they worry about the security and confidentiality of on-line services and contacts. Focused on the pursuit of commercial or political objectives, enterprises and governmental organisations are often inclined to regard the protection of privacy as an inconvenience. At the same time, there is a failure to recognise the potential benefits of taking privacy into account from the outset when designing information systems and processes.

Privacy is in fact a success factor. Whether one is concerned with running an electronic government help desk, checking the way employees use e-mail, police powers of investigation, exchanging medical data in connection with employee reintegration, passing on customer information to non-EU countries or selling address information for direct marketing purposes, commercial or administrative success cannot be obtained without ensuring that personal data is handled scrupulously and correctly. Because, unless privacy is adequately protected, it will not be possible to win the trust of the citizen or consumer.

Against this background, the Dutch Data Protection Authority (CBP) presented a study report entitled *Klant te koop, privacyregels voor adressenhandel (Customer for sale: privacy rules for list broking)* to the chairman of the DMSA, the direct marketing industry's representative organisation, at the latter's 2001 Direct Marketing Days. The report was intended to address uncertainties within the industry and to make it clear that the law allowed considerable scope for the buying and selling of address data.

Similarly, it was felt that greater clarity regarding the rules on the transfer of personal data would be beneficial to the business community, which has an interest in the smooth and lawful exchange of information with countries outside the EU. The CBP accordingly published its *Policy paper on transfers of personal data to third countries in the framework of the new Dutch Data Protection Act* in 2001. As well as dealing with the various issues in turn, the report explained the CBP's role in the permit process for the benefit of enterprises and organisations involved in the transfer of data outside the EU.

Privacy and ICT

In 2001, the CBP also conducted research into the threats to privacy and the opportunities for privacy protection associated with information and communication technology (ICT). The Data Protection Authority published a report entitled *Beveiliging van persoonsgegevens (The Protection of Personal Data)*, which provides a framework for organising information systems to comply with the Dutch Data Protection Act. During the course of the year, considerable exposure was also given to the privacy audit tools developed in collaboration with the public and private sectors for use in the assessment and auditing of information systems.

In addition, the CBP worked hard to publicise the benefits of privacy-enhancing technologies. Such technologies prevent the unnecessary processing of personal data in information systems, and thus serve to bring about *'privacy by design'*. One particularly futuristic initiative in this field is the European PISA Project, in which the CBP has been participating. PISA – Privacy Incorporated Software Agents – was set up with the aim of developing design specifications for autonomous software 'agents', whose 'owners' would be able to perform or authorise electronic transactions of various kinds while retaining control of their personal data.

In the near future, the Netherlands can expect to see the arrival of numerous public and private 'trusted third parties' (TTPs). As the issuers of digital identity certificates, these entities will play a key role. In 2001, the Data Protection Authority accordingly published a report entitled *Sleutels van vertrouwen (The Keys to Trust)*: an initial examination of the implications of the European Privacy Directive and the Dutch Data Protection Act for the TTP sector.

Electronic government

The degree of care exercised by government bodies and other institutions when exchanging personal data has sometimes caused the Data Protection Authority considerable concern. Particularly where a number of institutions exchange personal data on a collaborative basis, it is not always clear who is or may be the controller for which data processing activities. Under such circumstances, efficient data processing can conflict with the subjects' interests and may even be against the law. Before long, collaboration and data exchange between government bodies will have developed to the point where a formal information infrastructure exists. So in 2001, the CBP initiated an investigation of the privacy issues associated with 'electronic government', which will culminate in the publication later this year of a paper setting out its views.

Police records

The gathering of information and the maintenance of records by the police and judicial authorities can have far-reaching consequences for the privacy of the data subjects. The CBP therefore takes a keen interest in this field. The records kept by criminal investigation units (CIEs) represent a particularly serious threat to privacy. Nevertheless, the quality both of the registration activities and of their supervision remained disappointing in 2001. The CBP has, however, noted the gradual development of a willingness to improve matters on the part of the police and judicial authorities. Since the end of the year, a circular issued by the Minister of the Interior and Kingdom Relations has come into effect, requiring the introduction of (external) auditing.

Investigative powers

In the past, companies and other organisations were often asked or ordered by the police and judicial authorities to disclose or allow access to computerised personal data (regarding customers, for example). In many cases, however, such orders were unlawful. The companies in question were consequently placed in a difficult position. Having received numerous complaints, the Data Protection Authority wrote to the Minister of Justice asking for guidance in this area. The Minister has since spoken out against this form of information gathering.
In 2001, the question of police powers was considered by the Committee on the Gathering of Information in Criminal Investigations (the 'Mevis Committee'). The committee suggested that the police and the Public Prosecutions Department should be given extensive powers, enabling them to

Results secured in 2001

IN LAST YEAR'S ANNUAL REPORT, IT WAS ANNOUNCED THAT IN 2001 PRIORITY WOULD BE GIVEN TO SECURING THE FOLLOWING RESULTS:

- **Information campaigns**

Information campaigns linked to the introduction of the Data Protection Act were organised in collaboration with the Ministry of Justice and the Ministry of the Interior and Kingdom Relations. The Data Protection Authority took care of the campaign aimed at representative organisations in the various sectors, focusing on the particular needs of each industry.

- **Website & information material**

The CBP's website (www.cbpweb.nl) has been redesigned and made more accessible. Further improvements are planned for 2002. A comprehensive review of the information on the site has been undertaken, and additional material posted. All the authority's publications are available free of charge on the site.

- **Self-regulation**

A leaflet has been published to help organisations interested in appointing a 'data protection officer', as referred to in Sections 62 and following of the Data Protection Act. Several dozen registrations have since been received and processed. Assessment guidelines have also been drawn up for organisations that are considering the introduction of a code of conduct, as referred to in Section 25 of the Act, and a leaflet is now under development.

- **Data protection & PET**

The report *Beveiliging van persoonsgegevens (The Protection of Personal Data)* explains how a controller should go about providing appropriate protection, as required by Section 13 of the Data Protection Act. A separate leaflet has been produced, dealing with the use of privacy-enhancing technologies (PET). Preparations are also being made for a symposium on this topic.

- **Auditing**

In conjunction with representative organisations and market players, a system for assessing the quality of the data protection arrangements within an organisation has been developed. The products of

require businesses and government departments to assist their enquiries by providing information. The CBP has opposed such a move, however, arguing that statutory regulations are required to ensure that the rights of all interested parties are more clearly defined. Neither commercial nor governmental organisations are simply investigative extensions of the police or the Public Prosecutions Department. Investigative bodies need to show greater sensitivity in the way they handle information. The proposals presently under consideration would result in information being made available regarding many people who were not suspected of any wrongdoing; this would amount to a considerable extension of police and judicial authority, despite the fact that the bodies in question have so far failed to abide by the existing rules.

Confidential communication

If the Telecommunications Data Requisitions Bill were to become law, data concerning telecommunications would be categorically excluded from the constitutional protection afforded to confidential communications. The CBP has always contended that the legislature should be cautious about requiring telecommunications companies to retain data. The authority could not therefore support the government's proposal that Article 13 of the Constitution should be amended, as recommended by the Committee for the Assessment of Constitutional Rights in the Digital Age. The CBP felt that constitutional protection should not be restricted to the content of communications, but should extend to 'traffic data', i.e. information about the communications.

Worker supervision

ICT is increasingly prominent in the modern workplace. One consequence of this is that workers now make daily use of equipment – digital access cards, security cameras, GSM phones, RSI programs and other software – which lends itself to their own supervision. The monitoring of workers' e-mail and Internet use was a very topical issue in 2001. In its contributions to the public debate, the CBP emphasised that each organisation should develop a set of monitoring arrangements, tailored to its particular circumstances. For this purpose, the authority made a range of tools available, which will be offered to organisations again in 2002, but has not involved itself directly in worker supervision.

Occupational disability

During the course of the year, close attention was paid by the CBP to social security-related issues, particularly the reintegration of workers after

this project – *Quickscan, WBP Zelfevaluatie (Data Protection Act Self-evaluation)* and Raamwerk *Privacy Audit (Privacy Audit Framework)* – have been posted on the CBP website and put into use in the field. The possibility of setting up a certification system will be examined in the context of a follow-up project.

- **Data Protection Act reports**

In anticipation of the new Data Protection Act coming into force, special software was developed for use by anyone who has to report the processing of personal data to the CBP in accordance with the Act. With the software, the user can draw up a standardised report and submit it on diskette. The program comes with guidelines designed to help the user decide whether an activity is exempt from the reporting requirement. These guidelines can also be consulted on the CBP website. New report forms and explanatory information have also been developed.

- **Enforcement**

Provisional versions of the processes for issuing orders and imposing penalties have been developed and are now being introduced. The policies and principles that the CBP is to follow in the exercise of its powers in these areas will be published in the course of 2002.

- **Working methods and procedures**

The working methods and procedures that the CBP is to follow in the performance of its other duties and the exercise of its other powers have been defined and are being introduced in stages. The underlying principles and policies will be published in the course of 2002.

- **Third countries**

A policy statement on data transfers to third countries (as referred to in Sections 76 and 77 of the Data Protection Act) has been posted on the CBP website. A leaflet and information sheet on the same topic are also available from the site. Dutch and English-language printed versions are currently being prepared.

- **Management and organisation**

A management charter has been developed and since approved by the Minister of Justice. An organisational and staffing plan has also been drawn up, on the basis of which a system of competence management will be introduced.

Targets for 2002

THE MAIN RESULTS THAT THE CBP WILL PURSUE IN 2002 ARE AS FOLLOWS:

- **Electronic government**

The use of ICT can make the government more accessible, more effective and more client-oriented, while also reducing the administrative burden for companies and institutions. The CBP will publish a review of the privacy issues associated with electronic government, with a view to assisting the identification of promising solutions and opportunities for improvement.

- **ICT in healthcare**

Changes are also taking place in the healthcare sector, which could have far-reaching consequences for privacy protection. The CBP will seek to contribute to balanced progress in this field by preparing a publication devoted to the use of ICT in the sector.

- **Research and statistics**

As interest in results and effects increases, more scientific and statistical research is undertaken. The CBP will produce a framework document setting out the legal rules on the use of personal data in the context of scientific and statistical research.

- **Workers**

Privacy at work will be addressed, with the release of new versions of the report on the supervision of workers' use of e-mail and the Internet, and of the privacy checklist for staff councils. Preparations will also be made for the publication of information regarding the position of employees on sick leave.

- **Trade information**

Research has revealed a need for clarification of the legal situation as regards the processing of personal data by trade information agencies. The CBP will work towards the availability of clear guidelines on the lawful processing of personal data drawn up for use by those active in this field.

- **Telecommunications use**

The CBP will undertake exploratory research into the processing of

periods of occupational disability. The first structural changes took effect on 1 January 2002, when the SUWI (Work and Income Implementation Structure) Act came into force. The CBP urged the government to ensure the total transparency of the data flows associated with the Act. It should be clear to everyone involved – individuals, institutions and companies – just what information can lawfully be exchanged, between whom and for what purposes. Clarity in these matters can be achieved by the
careful formulation of regulations defining the permissible aims of information provision.

Increasingly, the occupational reintegration of people who have been unfit for work for extended periods is contracted out to private companies. When advising the government on various legislative issues, the CBP has repeatedly underlined the need for specific regulations – preferably based in legislation – covering the exchange of information in the context of reintegration activities. Someone who is being reintegrated is in a vulnerable position, and the data that is being exchanged is essentially of a medical nature. The evident conflict between the need to protect privacy and the need to help people back to work is such that the providers of reintegration services would benefit from guidance. To date, however, no such guidance has been made available.

Care referral

ICT is ever more commonplace in the healthcare sector. It is not only regional and national electronic registers and market forces that are relevant in this context; waiting lists and care referrals have also been the subjects of intense debate. Indeed, the collection and distribution of highly sensitive data are involved in both cases. In many instances, medical confidentiality is at issue. Furthermore, a patient's right to privacy requires structural protection. Otherwise, in a complex and rapidly automating sector where efficiency is prioritised and sizeable financial interests are at stake, the patient's need for care will tend to preclude the assertion of his or her right to privacy.

personal data concerning telecommunications use, in particular billing data. The findings will be presented at a workshop for experts and representatives of organisations active in the sector.

- **Special police records**

The police's control of the records of 'criminal investigations' could be improved, with a view to enhancing both privacy protection and the investigation of crime. The CBP would like to see better structural supervision of such records and more efficient arrangements for processing requests for access to such records.

- **Public register of WBP reports**

An open-access public register of data processing activities reported to the CBP in accordance with the new Data Protection Act (WBP) will be set up on the authority's website. An improved version of the software for submitting reports on diskette will be released and Internet reporting will be enabled.

- **Preliminary investigation**

Details of the experience gained with the preliminary investigation of processing activities that entail special risks (as referred to in Sections 31 and 32 of the Data Protection Act) will be published on the CBP website. Where possible, standards on common processing operations will be developed in conjunction with the interested parties.

- **Enforcement plan**

The CBP will create the conditions for the systematic monitoring of compliance with the statutory reporting requirements. These conditions will be described in an enforcement plan, which will also give details of various other activities in the field of supervision, investigation and intervention.