2008 in a nutshell

Last year, the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] was able to strongly improve its positioning as supervisor. Its chosen focus is the investigation of compliance with the rules concerning the processing of personal data and enforcement action where legislation is violated. In 2008, the Dutch DPA also make clearer choices, on the basis of risk analyses, on how to deal with the large number of very different subjects that it is confronted with. The Dutch DPA prioritises structural issues and violations that affect many people - vulnerable groups in particular.

The internet

Last year, the Dutch DPA received a large number of complaints and warnings about the publication of personal data on the internet. These relate particularly to requests for the removal of this data and to the rights that an individual has if his or her data is published on the internet. By taking enforcement action against websites that structurally violate the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act], the Dutch DPA wants to increase the alertness of both controllers and data subjects. Both parties must be more aware of the rights of data subjects and of the need for these rights to be respected.

Emergency action against a website containing the personal data of civil servants and politicians yielded success in record time: access to the site was blocked within just one day. Action against a municipality that published applications for planning permission complete with personal data and the signature of the applicant and the name and signature of the relevant official on its site led to the development of a new online application form that will be used throughout the Netherlands. As a result, the unlawful publication of this personal data has been stopped.
The covert registration of the IP addresses of visitors to the website Geencommentaar.nl [nocomment], with the object of making this list accessible to others, was declared unlawful by the Dutch DPA. In response, the controller stated that the list had been destroyed and the software removed from the site. The website beoordeelmijnleraar.nl [assessmyteacher]was also declared unlawful. The website holder subsequently made a number of changes to the site.

Together with the Onafhankelijke Post- en Telecommunicatie Autoriteit (OPTA) [Independent Post and Telecommunications Authority], the Dutch DPA was successful in its efforts to deal services that facilitate reverse searches – using a telephone number to find the corresponding name and address details – and in the specification of the conditions under which viral marketing is permitted.

At a European level, the Article 29 Working Party published a much anticipated Opinion on internet search engines, which was followed, in February 2009, by hearings with four internet search engines. Partly as a result of this, competition has developed between the search engines, with privacy friendliness as the key factor.

Business and work

Medical data on employees is of a very sensitive nature. Further to the investigation of an occupational health and safety service, the Dutch DPA suspects that other occupational health and safety services also structurally disclose these data to employers. Because of this, the decision was made to examine data processing by other occupational health and safety services as well. The investigation will be continued in 2009.
The greatest possible care must also be exercised where data relates to sensitive information about an individual's financial position. The Landelijk Informatiesysteem Schulden [National Debt Information System] submitted a design for a registration system to the Dutch DPA for assessment twice. The design was rejected by the Dutch DPA in both instances. Data processing had been demarcated insufficiently and the group of people with access to these data would be too large, which would entail the risk of damage to individuals who had been entered in the system erroneously.

One of the structural problems of privacy protection is that many people do not know where their data ends up and what happens to it. If persons are investigated, whether by a private detective agency or the afdeling Sociale Recherche [Social Security Fraud Department], these persons must be notified thereof when the investigation has been completed. Following its investigation, the Dutch DPA has established that this duty to disclose is still not complied with in many cases. The Dutch DPA will continue its vigilance in this respect.

Obtaining data that can lead to more efficient and conscious energy use must also occur in line with the Wbp. A number of privacy safeguards were added to the legislative proposal relating to the introduction of smart energy meters following criticism from the Dutch DPA.

Transport

After wrangling, which lasted for years, concerning the use of travel data for marketing purposes following the introduction of the OV-chipkaart [public transport chip card] and the publication of a study by the Dutch DPA on the use of the card on the Amsterdam metro network, the public transport companies eventually came up with a system that satisfies the requirements of the Wbp. The Dutch DPA will monitor the implementation and compliance with the standards laid down. An official investigation in 2008 into the processing of personal data for the purpose of the chip card, which will be compulsory for the Rotterdam metro with effect from 29 January 2009, led to the conclusion that there is no reason to take any further steps at this stage.

The kilometre price system may also lead to a detailed image of travel behaviour, in this case concerning individual motorists. The Dutch DPA has advocated data minimisation in the Lower House.

The monitoring of cars that use certain routes involves all citizens who drive cars, including those who have nothing to hide. The Dutch DPA has developed guidelines for Automatic Number Plate Recognition (ANPR), which are intended to bring an end to the lack of clarity on what is and what is not allowed in the implementation of this method. The police is not allowed to retain and process all scanned data. A situation must be avoided where all motorists are regarded as potential suspects.

Healthcare

Extra care and proper security are required when processing data on someone's health. In the legislative proposal that provides for the Electronic Patient File, consideration is given to the highly critical advice issued by the Dutch DPA in this respect. In principle, only professionals with a treatment relationship with patients will have access to their medical records.

The Dutch DPA points to the need for citizens, and patients in particular, to have the right to know who has access to their data, when and how and the right to know that this data is processed securely in other healthcare areas in which personal data is exchanged as well. This applies when health insurance companies provide data to the central administration office on insured parties with health problems who are eligible for an allowance. It applies when one insurer discloses personal data to another insurer when collective contracts are transferred. It applies for the national processing of data for care registration across the board under the Algemene wet bijzondere ziektekosten [Exceptional Medical Expenses Act]. It applies when issuing personal data to the College voor Zorgverzekeringen [Care Insurance Board] for the purpose of the collection of premiums for health insurance from defaulters. It also applies for the use of the burgerservicenummer (BSN) [Citizens Service Number (CSN)] in the healthcare sector: the processing and provision of personal data must comply with a certain level of information security.

Compliance with the level of information security required does not go without saying, as became evident from an investigation that the Dutch DPA conducted with the Inspectie voor de Gezondheidszorg [Healthcare Inspectorate]. None of the 20 hospitals investigated complied with this standard, which may have serious consequences for the quality of care provided and for patient privacy. The hospitals must demonstrate that they will comply with the standard and how they will do this.

Young persons

The digital processing of personal data in general and by the government in particular explicitly demands safeguards. This applies all the more where information relates to children and young persons.

In 2008, the Dutch DPA issued highly critical advice on the draft legislative proposal that would result in the creation of a Verwijsindex Risicojongeren [reference index for young persons at risk]. In the opinion of the Dutch DPA, the proposal is contrary to the Wbp. Criticism focuses particularly on the object of the reference index, which is insufficiently concrete and, combined with its unclear criteria for the registration of a young person by his or her care provider, entails an almost inevitable risk of arbitrariness. Although the legislative proposal submitted on

Second stage of evaluation of the WBP

- **The study report**

The objectives of the Wbp, namely to safeguard the balance between privacy interests and other interests and to strengthen the position of individuals whose data is processed, are not yet being achieved in full. This is the most important conclusion to emerge from the second stage of the Wbp evaluation study, the report for which was recently presented to the House of Representatives.

The second stage of the evaluation of the Wbp relates to the empirical part of the study on the effect of the Wbp. The *Wat niet weet, wat niet deert* ('ignorance is bliss') study report was completed at the end of 2008. The main study question is as follows: 'To what extent does the operation of the Wbp comply in practice with the objectives of the Act, particularly given the problems observed in literature, and which adjustments are possible and advisable within the context of the EU Directive?'

This problem definition has been elaborated on in 18 subquestions that have been studied by means of questionnaires, expert meetings and (in-depth) interviews, amongst other things.

According to the report, the Act has not really found its way into legal practice yet. The Wbp is an Act that is difficult to apply. It is noted in this context that the Wbp is still relatively new and that more time is needed for legal development, for the interpretation of the open standards laid down in the Wbp.

As regards the rights of data subjects, their right to access and correct personal data, it has been noted that only limited use is made of these rights.

Satisfaction varies concerning the Dutch DPA's performance of its duties. There is an appreciation, on the one hand, of the guidelines, advice and mediation that the Dutch DPA provides. However, on the other hand, even more is expected of the Dutch DPA in relation to the provision of information and advice. According to some, the choice made by the Dutch DPA in 2007, namely to focus on its supervisory task as one of the many tasks allocated to it, was made too early, given the lack of legal development. In other words more needs to be invested in knowledge development. However, according to the report, another line of thought is possible too, in which the decision to focus on supervision and enforcement will actually lead to the development of initiatives elsewhere in relation to information, awareness and clarification of (legal) norms.

- **Essay**

The Dutch DPA was of the opinion that (too) little attention is being given to technological developments in relation to the Wbp in the second stage of the evaluation. Because of this, it approached an academic, professor dr. Paul De Hert, a professor at the Vrije Universiteit Brussel and affiliated to the TILT at Tilburg University as a senior lecturer, in 2008, asking him to discuss this aspect in more detail in an essay. An abridged version of this essay was published on 28 January 2009, on the occasion of European Data Protection Day. An English translation of this essay is also available. The final version of the complete essay will be published later in 2009.

- **Judgment collection**

The observation made in the evaluation report to the effect that the Wbp has not really found its way into legal practice yet would seem to be belied by the *Uitsprakenbundel Wet bescherming persoonsgegevens* [Judgment collection in relation to the Personal Data Protection Act] to be published by the Sdu in April 2009. This publication, edited by both employees of the Dutch DPA and independent experts, actually includes a very large quantity of 'external' case law on the Wbp, in addition to recommendations and views from the Dutch DPA.

6 February 2009 responds to the criticism raised by the Dutch DPA – amongst others – in several areas, the essence unfortunately remains the same.

It is often claimed that privacy regulations prevent the proper implementation of child protection measures. This myth was dispelled during a round table conference in April 2007, between the Dutch DPA and professionals in the field of youth care. The Dutch DPA is able to agree to the draft legislative proposal on the amendment of the child protection measures that introduces a *right* to speak. If the interests of the child make it necessary to break (doctor-patient) confidentiality, the care provider must be able to exercise his right to speak.

Primary schools issue educational reports on their pupils to secondary schools. The Dutch DPA has investigated compliance with the information obligation to the parents of children in this situation. This is vital for the possibility of correcting the report, which can have a protracted negative effect on children if it contains incorrect or outdated information.

Police and the judicial authorities

The serious misuse of personal data in the form of identity fraud is also set to increase in the Netherlands. To combat this theft of someone's personal data, compliance with the information obligation is vital, so that the data subject knows that an organisation is processing his personal data and which data is concerned. In 2008, via meetings with experts and a study of literature, the Dutch DPA explored the different ways in which identity fraud could be prevented and combated.

Safeguarding the correct and transparent use of personal data is also vital in light of the increased powers that police and the judicial authorities have in relation to the processing of personal data. In 2007, the Dutch DPA took the view that legislation that opens up the possibility for a DNA family relationship investigation as part of criminal proceedings is in violation of the Wbp. The Minister took the criticism raised by the Dutch DPA into consideration in a second proposal in October 2008.

As regards the proposal by the Openbaar Ministerie [Public Prosecution Department] to extend investigation reports – through the use of the internet and telephone, for instance – the Dutch DPA advised on the inclusion of appropriate safeguards in order to ensure that these reports are protected from search engines and that any mistakes are rectified quickly. The A*anwijzing opsporingsberichtgeving* [Instructions on investigation reports] will be modified further to this criticism. The Dutch DPA also issued critical advice on the provision of criminal data from the Public Prosecution databases to data subjects and third parties for purposes not relating to the criminal procedure. The Dutch DPA feels that this is only allowed in certain cases and only where absolutely necessary. Advisability alone is not enough.

The Dutch DPA issued an investigation report on the internal exchange of personal data within the police forces via the police information desk. By far the majority of police regions were found to be completely unequipped for compliance with the requirements of the Wet politiegegevens [Police Data Act], which became effective on 1 January 2008.

International

Binding international rules for data protection are vital in order to cope with future privacy problems. At a worldwide and European level, more intense collaboration is necessary between

Brouwer Committee: transparency in registration is crucial

In January 2009, the Dutch DPA responded to the report by the Brouwer Committee entitled *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer* [Just do it; protecting safety and privacy].
The Dutch DPA agrees with the framework provided by the report, which is largely in line with the principles and provisions laid down in the Wbp. The view expressed by the committee, namely that transparency is crucial for a society of trust, is all the more compelling because recent research commissioned by the Dutch DPA shows that there are a worryingly large number of data files in which citizens are registered. "Citizens must know who, why, where and which data is being collected and used in relation to them", says Jacob Kohnstamm. The Dutch DPA also shares the committee's view that sound external supervision is a vital final element when promoting the careful use of personal data 'on the shop floor of safety' and that the government must provide the Dutch DPA with sufficient powers and financial resources to this end. According to Kohnstamm, this is currently not the case in a number of respects.
Contrary to the committee, the Dutch DPA believes that advice on legislation and regulations can and must go hand in hand with the supervisory task of the Dutch DPA. "Knowledge of and experience with the actual use of personal data that the Dutch DPA is gaining as a data protection authority, is yielding a vital seedbed for well-considered new legislation and regulations. What is more, abolition of the obligation to request advice on legislation is directly contrary to Article 28(2) of the European Privacy Directive. So, 'just keep on doing it', Kohnstamm says.
The duties of the Commissie veiligheid en persoonlijke levenssfeer [committee on safety and privacy], which is chaired by, mrs. A.H. Brouwer-Korff, mayor of Utrecht, include establishing what the Cabinet can do to ensure that care providers, prevention staff and crime fighters are able to exchange the data required easily and responsibly.

data protection authorities as is greater emphasis on the importance of data protection when making policy decisions in both the public and the private domain. These recommendations were made at the international conference of data protection authorities, which was held in October 2008. Attention is also being paid to the future of data protection legislation in a European context. Steps are being taken to ascertain how the Privacy Directive and its application can be strengthened.

Progress is being made in the coordination of approval of rules for the transfer of personal data by multinationals to countries outside the European Union. On the initiative of the Dutch DPA, a number of data protection authorities from EU countries have agreed to adopt each other's assessments of the codes of conduct adopted by multinationals for transfer – the Binding Corporate Rules. At the end of 2008, 15 data protection authorities had committed themselves to the mutual recognition of BCRs.

Moreover, last year, the European data protection authorities involved themselves intensively in checks on travellers and the passenger data issue, developments on the internet and judicial and police-related developments in the EU.

OBJECTIVES 2009

In 2007, the Dutch DPA decided to give more priority to enforcement action, in order to exercise its supervisory task and achieve the best results possible. In 2008, the Dutch DPA continued to work on the identification of investigation areas, based on problem and risk analyses, and on the organisational changes that would be needed as a result of this change in course.

As regards the *private sphere*, the Dutch DPA will commit itself in 2009 to the promotion of the use of personal data by both controllers and data subjects in line with legislation. Emphasis here will be placed on compliance with the duty of disclosure that rests on controllers.

In the *public domain*, the Dutch DPA will emphasise the obligation that the government has to be open and transparent. Authorities and implementers of public tasks must offer complete clarity as regards the use of citizens' personal data.

To be able to maintain this course, the Dutch DPA will continue to be very selective in its processing of individual cases and act primarily as a data protection authority. The organisation will continue to focus on:

- investigations into compliance and, where necessary, sanction imposition;
- the improvement of insight into technological developments;
- the improvement of supervision tools;
- the investment in public information.

The following concrete priorities have been determined for 2009:

Private supervision:

- Monitoring compliance with the Wbp and doctor-patient confidentiality by companies in the occupational health and safety service and reintegration sectors.
- Identity fraud. Complaints and warnings that point to violation of the Wbp will be handled with priority.
- In a European context, acting as a leading data protection authority when assessing the codes of conduct adopted by multi-nationals for the transfer of personal data to countries outside the EU (so-called Binding Corporate Rules).
- Supervision of compliance with the duty of disclosure that companies have towards consumers.
- Enforcement investigation into websites that structurally violate the Wbp, as announced in the *Richtsnoeren publicatie van persoonsgegevens op internet* [Guidelines on the publication of personal data on the internet], which guidelines were published in December 2007.
- Enforcement investigation into the unlawful provision of personal data to third parties by companies.
- Risk analysis of and investigation into evident violations in relation to the unlawful re-use of biometric data.

Public supervision:

- Completion of an investigation into the transfer of educational reports on pupils from a primary school to subsequent educational institutions and compliance with the duty of disclosure.
- Investigation into the processing of the Citizens Service Number or other personal data in national care registration by the College voor zorgverzekeringen [Care Insurance Board] under the Algemene wet bijzondere ziektekosten [Exceptional Medical Expenses Act].
- Follow-up investigation on the organisation of the police information desk at several police forces, focusing particularly on authorisation, quality requirements, logging and the role played by the privacy officer.
- Investigation into the effect of the Centraal Informatiepunt Opsporing Telecommunicatie (CIOT) [Central Information Point for Telecommunication Research] and requesting data stored with the CIOT.
- Local investigation of several regional Electronic Patients Files, for compliance with the applicable standards.
- Inspection of the security of data held by the Criminele Inlichtingen Eenheid (CIE) [Criminal Intelligence Unit), particularly where informants are concerned.
- Determination and publication of the final guidelines on the use of automatic number plate recognition, followed by an investigation into compliance with the Wet politiegegevens [Police Data Act] and the guidelines by police forces.
- Inventory of documentation available on and local investigation of one or more 'safe houses'.
- Investigation of camera surveillance in municipalities. This concerns both camera surveillance that municipalities carry out independently and camera surveillance carried out in collaboration with private parties.

International:

- Contributing to investigations into the operation of the European Privacy Directive (95/46/EC).
- Contributing to the development of initiatives with the objective of achieving a global standard for data protection and a global standard for company accountability.
- Contributing to theory development on the issue of applicable law from Directive 95/46/EC in connection with the increase in cases with a cross-border dimension.
- In addition to its usual participation in international forums there will be attention for trans-Atlantic relations, the London Initiative meetings, the spring conference of European data protection authorities in Edinburgh and the international conference for data protection authorities in Madrid.