Summary of the Annual Report 2009 of the Dutch DPA

Foreword

The endless possibilities of technology have offered individual people and society unprecedented advantages we had never dared to dream of until recently. The Internet, mobile telephony, RFID, social network sites, biometrics, cloud computing, and such like have brought dramatic improvement and change in everyone's lives and in the organisation and services of the market and the authorities.
One of the consequences of these changes which have often been deemed unavoidable is the fact that we all leave digital traces of our doings. Add this to the by now equally endless possibilities for storage, linking, and processing of all sorts of data, and a Kafkaesque situation is the inevitable result: we have no idea about what is happening to our data, with whom they finally end up, how and where which profiles are made, and what - possibly decisive - influence all this has on legitimate individual choices and the scope to develop one's abilities.

There are at least three important possibilities to react to these developments.

The first possibility is to use the same technological developments to minimise the chance of intrusion on a person's privacy; in jargon called 'privacy by design'. There is, for instance, a fundamental difference between a box in a car for the purpose of kilometre price that is continually transmitting location data to a central database by air or a box that is developed in such a way that all data remain in the car with the motorist keeping control of releasing those data.

It is evident that companies and authorities will always want to employ brains for the development of new, quick, efficient, and profitable products and services. It is, however, also in the interest of the final success of many of these products and services to give these brains the instruction to develop these products in such a way that they do not intrude on a person's privacy or do so much less.

The situation is too often such that those who dive into new technological developments involving the processing of personal data are often blind to the fact that this technology could also be used to provide safeguards to protect and secure personal data already in the development phase of a new product or service. It would be a good thing if the new Dutch government that is to be formed after 9 June 2010 would be steering to a course improving or obliging the use of privacy by design.

A second possibility to avoid a Kafkaesque situation somewhat may be found in the provision of information to citizens about the question of who is storing and processing which data about them and where and why. In order to be able to exercise their rights in the area of the protection of personal data, it is essential that citizens have this information available, so that they will not be confronted unexpectedly by particular data that were stored and processed in a completely different context.

Finally citizens also have the right to know and the interest in knowing whether the databases in which their personal data are processed, have been secured adequately against illegitimate consultation and against theft, loss, and abuse. Patients who visit a hospital must, for instance, be able to rely on the fact that their medical data are in safe keeping there. An adequate risk analysis must, for instance, have been conducted for the purpose of information security. If the private and public sectors fail in providing this security, this may result in major accidents, identity fraud, or data leakage; reason why the obligation of data breach notification should apply to all sectors in society.

Protection of personal data is not merely a fundamental right aimed at the individual. At the end, protection of personal data is to serve an important collective interest in a democratic society: being able to trust each other. Customers must be able to trust business and industry and citizens must be able to trust the authority. Seen in this light, privacy by design, increased transparency about who is doing what and why with our personal data, *and* adequate security of these data are the alpha and omega to avoid Kafkaesque estrangement.

J. Kohnstamm
Chairman

Main themes

The Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act] is currently subject to evaluation. In view of the possible revision of the Act the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] has stressed the importance of strengthening the position of data subjects. They should easily have access to information about why their personal data are processed, which measures preventing illegal use of those data have been taken and how they can exercise their rights. Apart from that, easily accessible complaints procedures should be developed / introduced, as well as the possibility of class actions.
As to the position of the controller, a shift is taking place from ex ante supervision to ex post supervision. Controllers should invest more in complying with the law and should have to pay for non compliance. The Dutch DPA propagates more transparency, a requirement to report data leaks and the use of privacy by design.
Thirdly, the position of the supervisory authority itself should be strengthened.

Next to its work as an advisor of the government concerning new legislation effecting privacy, the Dutch DPA in its supervisory role has opted to give priority to enforcement in the conviction that by doing so, it is able to make the most effective contribution to the promotion of compliance with the Wbp. For the purpose of establishing the priorities for 2009, a risk analysis was made of the processing of personal data in different sectors of society. The Dutch DPA subsequently selected cases which contained indications of serious violations of the law, which were structural in nature, affected many citizens, and against which the Dutch DPA had the power to take action. The Dutch DPA also kept its eyes open to topical events in the course of the year. The investigations and interventions carried out by the Dutch DPA (108 in 2009) did not only achieve results with individual controllers, but also appeared to have indirect effects.
The thematic 'guidelines' for 2009 entailed the obligation to provide information on and transparency about the transfer of personal data to third parties.

Major issues

The internet

After an investigation into the Internet company Advance the Dutch DPA concluded that the company had violated the law by collecting sensitive data of people using Internet platforms and subsequently selling their profiled personal data to third parties without having informed the persons concerned about this clearly and fully. At the time, approximately 2.2 million people participated at Advance's Internet sites. Advance offered them the possibility to complete a test, for instance, to find out 'your real age'. The investigation revealed that Advance had collected and processed, among other things, medical data,

whereas this activity is in principle subject to a statutory prohibition. Advance had not informed the persons concerned about the use of their data in accordance with statutory requirements.

A site used to assess teachers by their pupils caused serious damage to the privacy of the teachers concerned. Following investigation by the Dutch DPA the site was adapted and shielded from search engines.

The Dutch DPA also investigated two sites aimed at young people. The social networksite www.zikle.nl was required to inform its users adequately about the goals for which personal data were collected and processed, to apply security measures and to shield pages containing personal profiles. Www.jiggy.nl used a game to entice users to hand over email addresses of other people for direct marketing purposes. After investigation, the proprietor of the website removed the game.

Financial data

After the introduction of the instrument of an Advisory Letter in 2008, the Dutch DPA drew up its first advisory letter in 2009 at the request of the Stichting Landelijk Informatiesysteem Schulden (LIS) [National Information System of Debts] which was followed by a second advisory letter in response to a new draft of the LIS. Tests conducted by the Dutch DPA revealed that neither of the drafts complied with the statutory requirements. With respect to the second draft, the Dutch DPA concluded that the draft far exceeded the original purpose of the draft, i.e. the registration of overdue debts to avoid problematic debts. This may result in the fact that a substantial group of people will be registered who do not belong in the register but who will be confronted with the negative consequences of being reputed as a problematic debtor.

A bank passed on young clients' account numbers and addresses to a charity, without informing the clients or asking their consent. Following a complaint the Dutch DPA investigated the matter, which led to adaptation by the bank of its routine.

In 2009 the Dutch Finance Minister followed the DPA's advice on legislative proposals for the establishment of a pension registration. The idea is that each citizen can check his or her retirement pay rights on line. As these data will undoubtedly attract other parties, the Dutch DPA pointed out the necessity for tight security measures.

Medical data

On the basis of investigations at two current regional electronic patient records systems (reprs), the Dutch DPA established that the Wbp had been violated. The Dutch DPA initiated compliance procedures against both reprs. These procedures resulted in the fact that one of the two reprs ceased the unlawfulness established, by, among other things, informing all patients personally about the inclusion of their data in the reprs.
Proposed legislation on electronic patient records continued to cause concern. Critical advice of the Dutch DPA on the initial legislative proposal in 2007 led to adaptation of the draft. Amendments by the House of Representatives however made it possible in some cases for health care insurers to have access to patient records. The Dutch DPA advised the minister to delete this exception to the general prohibition. The Minister has indicated he will follow this advice.

Another cause for concern regards information security in hospitals. Investigations carried out by the Dutch DPA and the Inspectie voor de Gezondheidszorg (IGZ) [Netherlands Healthcare Inspectorate] in 2007 and 2008 revealed that none of the twenty hospitals investigated complied with the standard

for information security. In 2009, the Dutch DPA imposed orders subject to a penalty for non-compliance on four hospitals that still had not properly organised this aspect.

Investigation into the procedures of a number of occupational health and safety services resulted in the conclusion that at least one service – Tredin – acted systematically in violation of the law by providing medical data of sick employees to their employers whereas these data were subject to medical confidentiality. The Dutch DPA imposed an order subject to a penalty for non-compliance on this health and safety service in 2009. The health and safety service subsequently ceased the violations within the compliance period set. The investigation into three other occupational health and safety services has been continued.

Other activities in the private sector

We might seem to get used to it, but supervision by camera remains a far-reaching means, about which the Dutch DPA receives a lot of questions from citizens. The Dutch DPA investigated the use of camera surveillance in an industrial estate. The findings were generally positive for the company that is responsible for the surveillance. The company promised to change the rules on inspection in order to make them consistent with the requirements of the Wbp.
Because it isn't always clear if private companies or government bodies are responsible for camera supervision, the Dutch DPA has decided to develop new Guidelines on the subject.

A lot of buzz was generated by the proposed introduction of the so-called 'smart' electricity meter, which can provide a very detailed picture of someone's household and thus also of the periods people aren't at home. Consumers should be allowed to make informed choices regarding the frequency and amount of information that can be collected. The draft bill has been amended following the Dutch DPA's advice to the Minister.

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]. Criticism focused 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 6 February 2009 responds to the criticism raised by the Dutch DPA – amongst others – in several areas, the essence unfortunately remained the same. In 2009 the Dutch DPA was asked for advice on a number of executory measures the new bill entails and again, warned for arbitrariness.

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. More than half of the schools that were investigated did not record if the parents were informed or not. Following the investigation the Dutch DPA issued Guidelines for primary schools on the subject.

Police and the judicial authorities

Safeguarding the correct and transparent use of personal data is vital in light of the increased powers that police and the judicial authorities have in relation to the processing of personal data. In 2007 / 2008, the Dutch DPA investigated 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 (Wpg) [Dutch Police Data Act], which became effective on 1 January 2008. In 2009 a follow up investigation in three regional police forces showed that, setting aside differences, none of the forces complied fully with the requirements for authorization and monitoring.

Intelligence services can compare their information directly with police records. In an advice regarding proposed legislation on this independent form of consult of police databases the Dutch DPA has asked the government to make clear why this large scale consultation is necessary.

In 2009, the Dutch DPA developed guidelines for the purpose of automated number plate recognition (ANPR) by the police. In these guidelines, the Dutch DPA explains which interpretation of the statutory standards it maintains as a supervisory authority in exercising its powers. Later on in the same year, the Dutch DPA conducted investigations into the application of ANPR by two police forces and concluded that both police forces knowingly acted in violation of the Wpg by processing no-hits 120 or 10 days, respectively. A no-hit means that a scanned number plate does not occur in the reference file and that this number plate is
consequently not sought by the police. The registration of this number plate must be destroyed immediately. In response to the publication of the final investigation findings, both forces announced at the beginning of 2010 that they would cease the unlawfulness.

Passengers who want to participate in a system allowing for automated border passage, for example by means of an iris scan or fingerprints, have to be screened beforehand. The Dutch DPA has asked the Minister of Justice to make clear which starting points will be used in these background investigations.

International affairs

The processing of personal data doesn't stop at the border. In order to develop a high level of protection to personal data elsewhere, effectively harmonized supervision is required. That calls for a common policy and co-operation with the other Data Protection Authorities in the European Union and in the rest of the world. Chairman Kohnstamm visited the U.S.A. in November 2009 to discuss possibilities for a constructive dialogue between Europe and the US about their different approaches to privacy protection.
In various European fora the future of the Privacy Directive of 1995 was discussed. The Article 29 Working Party (WP29), which as of 15 February 2010 is chaired by the Netherlands, concluded that the basic principles of the Directive remain valid, but that the practical implementation of the rules could be strengthened and modernized. This could be done for instance by clarifying the application in practice of principles as transparency and consent and by introducing supplementary principles like privacy by design and accountability.
The International Conference of Data Protection Authorities convened in Madrid in November 2009. Supported by, among others, the Dutch DPA, the Conference adopted a resolution on the drafting of international standards for privacy and data protection.

Apart from the revision of the European Directive, WP29 concerned itself with social networksites, the protection of children, pre trial procedures, the duty to report dataleaks and a common European view on treaties with third parties on fingerprints and DNA databases.

The Dutch DPA supervises the national parts of several European systems for co-operation by police forces and judicial authorities. These include for instance Europol and the Schengen Information System.