# Translation of Foreword and Introduction of the Dutch DPA Annual Report 2011

## The Dutch DPA in 2011

**Everyone is entitled to careful handling of his or her personal data. Increasing digitisation and globalisation means that the number of instances of data processing is growing incessantly. In this context, it is all the more important that companies and governments only collect and use personal data of citizens in accordance with the law.**

**The Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] supervises compliance with statutory rules that relate to the protection of personal data, if necessary with the use of sanctions.**

**The Dutch DPA also advises the government on intended legislation that relates to the processing of personal data.**

**In the performance of its activities and when rendering account in respect thereof, the Dutch DPA takes into account the social context of the questions, problems or complaints presented to it. As the case arises, the Dutch DPA cooperates with other data protection authorities, both at the national and international level.**

**FOREWORD**

When power combined with the use of personal data leads to uncontrolled and unjustified influencing of the free development of people, data protection authorities worldwide have to take heed and intervene where necessary and possible. The nearly boundless opportunities now offered by technology for distinguishing one individual from another demand full attention in that connection.

Profiling by making use of the enormous amounts of data available as a result of IT and the Internet combined with the use of the latest calculation methods (algorithms) can bring many benefits both in the private and the public sector.
Companies can ensure that consumers receive only advertisements and offers that are interesting to them: no more spam but customisation.
It is conceivable in the public sector that the government, as a result of this technique, will be able, on the basis of a well-considered risk profile, to contact, at an early stage and in a targeted manner, persons who are seriously at risk of going off the rails in a social sense. The effectiveness of these forms of profiling and the chance of incorrect conclusions demand some caution for the time being; it is up to science, technique and practice to bring an end to these uncertainties.

However, profiling also has an undesirable side from a social perspective. People are assessed and treated in a certain way on the basis of profiles. Automatic decisions can be linked to those profiles, which could include the exclusion from a service and a tightening of checks. In addition, for citizens profiling is a process that is as opaque as it is inscrutable. Moreover, it is possible to generate a profile of a citizen or consumer from search behaviour on the Internet and on the basis of the information that can be derived from websites that have been visited. That citizen or consumer is consequently presented, without noticing and without asking for it, with only as it were 'censored information'. Other relevant information and options are withheld from him (the 'filter bubble'). This means that profiling can lead to stigmatisation and discrimination and to a society in which free choice has become illusory.

In order to gain optimum benefit from the positive sides and combat the negative sides as effectively as possible, it is necessary, now more than ever, to strengthen the position of citizens and, for this purpose, to strengthen several of the principles that are at the basis of the protection of personal data. These concern in particular the principles of purpose limitation, data minimisation, explicit consent as the basis for processing of personal data, security, transparency and effective enforcement.
In addition, companies and institutions have to be encouraged to take those principles into account as early as the development stage of products and services involving the use of personal data and to be transparent about what data they hold on which persons, why they hold that data and where they store it.

And finally, strengthening the position of the data protection authority is essential, both as regards its powers and in the field of staffing.

The ongoing 'review' of the new privacy legislation and regulations that is currently in progress at the EU, the Council of Europe and the OECD offers an excellent opportunity to suit the action to the word and to adjust legislation accordingly.

Jacob Kohnstamm
Chairman of the Dutch Data Protection Authority

## INTRODUCTION

**Confidence in public institutions and in businesses is one of the foundations of our society. It is therefore very important that citizens and consumers in a digitised living and working environment can have confidence in the manner in which their personal data is processed. Everyone has the right to know who does what with his/her data and why.**

In the past year, the Dutch Data Protection Authority ( DutchDPA) [ College bescherming persoonsgegevens (CBP)] focused on the correct provision of information to those whose personal data are being processed, both in the public and in the private domain. Below a selection from the various activities of the Dutch DPA in 2011.

*Public sector*
In 2011, the Dutch DPA's attention in the public sector focused mainly on reliable government. It is very important for the government that citizens have confidence in the performance of public institutions. This means, however, that citizens who entrust (sensitive) personal data to the government, whether they are obliged to do so or otherwise, can rely on the fact that the government also supervises the careful handling of these data and secures it sufficiently. It is essential in this context to ensure as much openness as possible and a sufficient information provision. Citizens have to know what personal data is being processed and for what purpose, irrespective of whether this is done by schools, social services or the police.

For example, in its recommendations concerning intended processing and the exchange of student details, the Dutch DPA emphasised that it has to be substantiated each time in that connection why including those, sometimes sensitive, data is necessary to supervise students adequately. Recorded data accompany students throughout their school career and can attach a harmful label on a student. Schools also have to provide clear information on how students or their parents can exercise their rights on the basis of the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act].

The importance of the proper provision of information was also evident from investigations performed in 2011. For example, the investigation performed by the Dutch DPA into file linking by the Social and Intelligence Investigation Service (SIOD) showed that the SIOD has acted contrary to the law, inter alia, because the Service did not inform people of the processing of their personal data within the context of investigating social security fraud.
The SIOD also stored personal data for longer than is necessary for the objective, namely combating fraud.
Storing personal data also applied in the aftermath of the investigation the Dutch DPA performed previously into the police storing number plate details obtained automatically. The Dutch DPA concluded at that time that these data has been stored for too long, which meant that all passers-by wound end up in a police register unnecessarily. A legislative proposal subsequently submitted for debate by the Minister of Security and Justice should provide a legal basis for a term of retention of one month. The Dutch DPA finds that the need for such a long term has not been demonstrated. Considering all car drivers in advance to be potential offenders cannot be justified, nor can considering all applicants for benefits to be potential fraudsters.

Investigation into the manner in which assistance and information points of the Tax and Customs Administration, intended to provide advice to citizens who wish to apply for care, housing or child care benefit, request data from the Tax and Customs Administration, showed that this occurred without the consent of the citizens involved. Data security was not sufficient either. The government itself should therefore check whether personal data is processed correctly. This can be done by performing regular audits. The Police Data Act, which entered into effect on 1 january 2008, contains an obligation to have an external audit performed within two years after the effective date of the act and to send the findings of the audit to the Dutch DPA. The Dutch DPA's investigation showed that none of the police forces or the special investigative services had complied with this obligation in time. Police data are sensitive data that have to be handled with a great deal of care. Being incorrectly registered as a suspect or offender, or having unauthorised persons gaining insight into his or her police file, can have serious consequences for those involved. It is therefore important that the guarantees for said careful use are left in place.

*Private sector*
The landscape in which personal data is processed has changed from a clear overview of a number of large databases into a tangled system of national and international companies that offer complex services. It has become impossible for average consumers to follow what parties process their personal data, to whom they provide it and for what purpose. Companies should not just simply assume that people have granted their consent for a certain type of data processing. They have a statutory obligation to inform citizens thereof and to enable them to exercise control over the use of their data. Moreover, data has to be secured properly.

The investigation into the manner in which Internet giant Google used Street View cars to collect data on Wifi routers led to Google promising that in future it will offer Internet users worldwide an opt-out option which will allow them at all times to object effectively and without cost against the processing of data concerning their Wifi routers. Moreover, the company promised, as was demanded, to inform, both online and offline, the parties involved of the collecting of Wifi router data using Street View cars for the purpose of its geolocation service and to furthermore irreversibly delete the already collected SSIDs (the network names of the Wifi routers).

Following Dutch DPA action, TomTom also promised to bring its information to its clients in line with the statutory requirements by February 2012. TomTom collects geolocation data of users of its equipment. Geolocation data provides a penetrating picture of someone's actions. The conclusion of the investigation the Dutch DPA performed at TomTom was that the company did not provide the users of its devices with sufficient information concerning the question of what the company exactly does with those data, such as providing targeted information about traffic jams on the road.

The extensive media coverage about data breaches and insufficiently secured databases show all the more that companies have to secure their systems adequately. Pursuant to signals and announcements in the media, the Dutch DPA performed investigations at fifteen companies into the measures they take to secure their processing of personal data. Organisational measures are required in addition to technical measures. These have to be secured in an information security plan or a contract or a service level agreement with those processing personal data. Should a data breach nevertheless occur, it is important that this is communicated. The Dutch DPA is very much in favour of an obligation to notify data breaches and is preparing for checking compliance with such an obligation once it is introduced by law.

*International*

Data processing does not end at the border. In a European and global connection, there is increasingly more intensive cooperation between national data protection authorities, both in preparation for a new European framework of privacy legislation and as regards joint supervision of the transfer of personal data by multinationals, and when taking up positions concerning the conduct of large parties.

In the past year, the so-called Article 29 Working Party of the data protection authorities in the countries of the European Union adopted a joint position concerning the central concept of 'consent' from the European Directive. Furthermore, it rendered a negative judgment in an opinion issued in December 2011 concerning the code of conduct of the trade organisations in the online advertising industry. Other subjects with which the joint data protection authorities occupied themselves are location data, passenger data, data concerning bank transactions and agreements with the US, the Eurodac fingerprint system and a code of conduct for RFID tags. In an institutional sense, a great deal of attention was devoted to future European regulations. Towards the end of 2011, the Dutch DPA announced its provisional position concerning proposals for a new, comprehensive privacy Regulation, which is intended to replace the current Directive, and concerning the Directive concerning cooperation between the police and the judiciary and the related exchange of data.