Foreword

The protection of personal data increasingly gets a place in the spotlights. “Dummy spies on customers” (Spits); “Confidential information lost due to leak in terminal equipment” (Trouw); “Municipalities careless with private information” (NRC); “Albert Heijn knows more about us than the mayor” (Volkskrant), these are just some examples of the numerous newspaper headlines in 2012.

Citizens are often insufficiently aware of the possible consequences of the collection and use of their personal data. It is therefore often a big shock – also for those who say they have nothing to hide – when it turns out that the information provided in good confidence is lost, or makes it impossible to live your live unmonitored without any justification.

The reactions of both government and the business community nonetheless give reasons to be hopeful. For example, in the business community there are proposals on the table to make privacy a ‘unique selling point’. As regards the government, the agreement reached by the governing parties in our government gives high priority to the protection of personal data: there is going to be a substantial penalty on the unlawful collection and processing of personal data.

Also at European level important steps have been made in 2012 to modernise the legal framework of data protection within the European Union. In January 2012, the European Commission (EC) presented its proposal for a new legal framework with the aim of strengthening, improving and simplifying the protection of personal data. Discussions in the European Parliament (EP), in the Council of Ministers (CM) and subsequently between all three institutions (the EC, the EP and the CM) on the proposals for new binding legislation are on-going at the moment of writing. The discussion on certain aspects of the proposals are however worrying, because some seem to argue for a substantial lowering of the level of personal data protection, even below the level we have today.

In the EP for example, proposals have been tabled to have a narrow definition of personal data and also to allow consent to be given implicitly, when consent is used as a legal basis for processing operations.

Furthermore, the principle of purpose limitation, one of the cornerstones of data protection, is under fire. This principle ensures that further use of personal data is only allowed when the purpose for further using the data is compatible with the original purpose of the collection and processing of that data.

But also with regard to the discussions in the Council of Ministers there are some concerns, in particular with regard to the plan to create greater flexibility for the public sector in the application of certain provisions of the proposed EU Regulation.

Naturally, different standards apply to the law enforcement sector than to the private sector. In the event of a reasonable suspicion of a crime, the law enforcement authorities actually have a duty – within the limits of the law – to process all necessary personal data! This is the reason why a separate Directive has been proposed specifically for the law enforcement sector. But the government consists of more than only law enforcement authorities, there are many other areas in which there is a relation between the government and its citizens, for example in the area of taxation, social security, education and public transportation .

The proposed Regulation currently already allows some flexibility for the public sector, which is justified, but in the negotiations in the CM some Member States – including the Netherlands – argue for even more flexibility for the public sector. The Dutch DPA, together with other data protection authorities in the EU have concerns about this for three main reasons.

First of all, the government probably is - by far - the greatest collector of personal data. Moreover, citizens are often obliged to provide their personal data to the government on the basis of legal requirements. Noblesse oblige: the government, especially, should adhere to the requirements and conditions that are essential for the protection of personal data.

Secondly, technological developments in combination with the wish to fulfil public tasks more efficiently and in a more customer-friendly way, may lead to the risk of 'function creep'. The digital haystack, which is perhaps already under construction due to the aforementioned developments, can easily be used to make all kinds of links between different databases, contrary to the principle of purpose limitation. The intention to give the local governments all kinds of tasks that are currently done by the central government, is very likely to increase this development. For citizens (and possibly also government itself) it will be almost impossible to know what data about whom is processed where and why, thereby risking that another essential objective of personal data protection – that of transparency – to 'flexibly' disappear from sight.

Thirdly and finally, the protection of personal data in the EU is a fundamental right. Fundamental rights primarily govern the relationship between government and citizens – certainly from a historical perspective. Allowing greater flexibility for the public sector in the application of the provisions of the Regulation could lead to the strange situation that the fundamental right of the protection of personal data only fully applies to the private sector and not in relation to the public sector.

The discussions and decision-making regarding the new data protection legal framework in the EU, presented in 2012, will continue and increase in intensity in 2013. All the different interests and arguments will have to be considered carefully. The final text of the Regulation however must ensure the protection of the fundamental right to data protection, applicable to both the public and the private sector.

Jacob Kohnstamm
Chairman of the Dutch Data Protection Authority

Introduction

Profiling, adequate protection of medical data and data security were the important points of attention for the Dutch DPA in 2012. The Dutch DPA paid particular attention to the manner in which businesses and organisations informed the public about data processing and – insofar as this is prescribed by law – ask consent for this.

Many people do not have a clear picture of the nature and consequences of the (re)use of their personal data which is increasing rapidly under the influence of the expanding technological possibilities. That is why in the past year, the Dutch DPA's efforts have been focused particularly on revealing data processing practices of which the public is usually unaware. Of the legal grounds on which personal data may be collected and processed, the ground of consent is often the weakest link. That is why in many of its investigations, the DPA examined whether the legal requirements for consent to be valid consent, were met.

A selection of the activities of the DPA in 2012:

Profiling and marketing
From public statements it appeared that Albert Heijn intended to create personal profiles of customers on the basis of their purchasing behaviour in order to provide them with personalised offers. The Dutch DPA concluded, after investigating, that Albert Heijn had not obtained valid consent from the customers because it did not meet the legal requirements . Another investigation conducted by the Dutch DPA showed that the Dutch Railway company (NS) kept detailed records of the travel behaviour of public transport chip card holders (OV-chipkaarthouders) and subsequently used this information for marketing purposes without asking the required consent for this from the travellers.

Medical data
During the disquiet unrest which arose around after the filming of patients at the emergency room department of the VU University Medical Center, the consent requirement played an important role. The DPA concluded that producer Eyeworks had not obtained legally valid consent for shooting these images as the patients had not given their unequivocal, express prior consent based on proper information. Given the particular situation it was also impossible to give legally valid consent: the patients found themselves in an extraordinarily dependent position, namely at the accident and emergency department needing urgent assistance.

In another investigation, the DPA concluded that Youth Care Agency North Brabant (Bureau Jeugdzorg Noord-Brabant) collected psychological test results of employees without valid consent. The employees were unable to give their free consent, because if they refused to cooperate with a test, the employees risked being fired.

In 2012, the Dutch DPA conducted an investigation with regard to the internal access to patient files at various care institutions. At a number of those institutions it turned out that inadequate security measures had been taken to ensure that only authorised hospital employees had access to the electronic patient files.

Data security
Data security was an important theme for the Dutch DPA in 2012. It therefore paid a lot of attention to investigating (possible) data breaches. The data breaches investigated often concerned situations where people were asked to fill in personal information on a web form

which was subsequently sent via the internet without adequate security measures. The security aspect also played a large role in an investigation into Whatsapp, a popular app for smartphones which can be used to send messages, photos and videos. The security of the app was below standard on several points, amongst others because Whatsapp sent the messages without encryption. This allowed third parties to intercept their content in an understandable format without the original 'whatsapper' being aware of this. As a result of the investigation, WhatsApp took immediate measures to encrypt the data traffic.

During this investigation the DPA also noticed that users of WhatsApp are obliged to grant access to the complete address book on their phone. The consequence is that the company collects all telephone numbers in those address books, including the numbers of contacts who do not use WhatsApp themselves. Users are not able to choose to only pass on numbers of contacts with whom they actually want to whatsapp. This means that both WhatsApp users, but also people who not use the app, have no control over which data they want to share.

International cooperation
At international level, in 2012 the Dutch DPA focused on strengthening the effectiveness of the supervision of personal data protection by collaborating with EU and non-EU data protection authorities. Globally operating controllers require cooperation also on a global scale. The investigation into WhatsApp was carried out together with the Canadian privacy supervisor. Together with its EU counterparts, the Dutch DPA carried out an investigation into the new privacy conditions of Google. The new policy appeared to be in violation of the European legislation on several points, partly because Google did not ask permission for the linking of certain personal data.

This publication only concerns a selection of the investigations and legislative recommendations made by the Dutch DPA in 2012. An extensive annual report has been published on www.cbpweb.nl. More information regarding the work carried out by the Dutch DPA can be found on this website and on www.mijnprivacy.nl, the public website of the DPA.