DUTCH DPA ANNUAL REPORT 2010

FOREWORD

A lot of hard work on the renewal and improvement of legislation and regulations in the field of the protection of personal data is being performed these years in nearly all national and international forums that are relevant to us. The Dutch Cabinet that took office last year will present a renewed Dutch Personal Data Protection Act this year in line with the intentions of the previous Cabinet.
The European Commission, the Council of Europe, the OECD, the Federal Trade Commission and the Department of Commerce in the US: all are busy translating new insights regarding the protection of personal data into existing practice or regulations.

The main driver of all these activities is the need to review the protection of personal data against the background of technological developments. As a consequence of those developments, nearly everyone engaged in normal daily social traffic leaves behind a large number of digital traces. And the pressing question is: how can the fundamental right to protection of personal data in the private and public sector be served best in present day?[*]

To answer that question, it is good to mark time and consider the influence the three defining main actors can or should have on the realization of that fundamental right: the individual, the organisation that collects or processes those personal data (in professional language referred to as the 'controller') and the supervisor.

In the legal system of countries that are ruled democratically, the individual citizen holds the most important position in situations in which choices have to be made: he or she should be able to determine – at any rate in theory – which data belonging to him or her are processed where, when and for which purpose. As a consequence, all sorts of guarantees have been included in European legislation and regulations in the field of the protection of personal data, so that citizens have and maintain insight into and influence on what happens with his or her personal data (consent, right of access, rectification and blocking).

The nearly limitless opportunities currently offered by technology to store and process data have consequences for the division of duties between citizens and the controller when it comes to the protection of personal data. Developments such as cloud computing, behavioural advertising and profiling in private and public sectors have led to the situation that individual citizens are hardly able to get a grip on who knows (or thinks he knows!) what, where and why about him or her. That is why the obligations imposed on controllers to comply with the principles of privacy legislation and regulations have to be strengthened in a practical sense. In other words: it seems as if 'informed consent' on the part of the

[*] *In a speech held by Madeleine McLaggan, member of the Dutch DPA, at the occasion of the conference 'Wbp in beweging – de toekomst van privacywetgeving', organised by Vereniging Privacy Recht, which took place on 24 March 2011, she deals with a selection of principles that form the basis of privacy legislation and which is and continues to be influenced by technological developments. How tenable are these principles in the information age and what does this mean for the working methods and role of the Dutch DPA as supervisor? It concerns the notions of personal data, transparency, consent and limiting use to a specific purpose, focusing on the provision to third parties.*

individual citizen is becoming an illusion as a result of technological developments. This should in no way lead to the conclusion that 'consent' as basis for processing personal data should be written off. The correct conclusion would be that the guarantees controllers should implement for the purpose of the careful use of personal data should be tightened. Because partly as a result thereof, consumers – both individually and collectively – and the supervisor will be able to monitor compliance with the principles of the protection of personal data considerably more vigorously. This will also make it possible to fill the gap that was created as a result of the situation that giving 'informed consent' has become nearly illusory. Necessity, data minimisation, purpose limitation, security and transparency together form the decisive elements for this purpose. In order to do justice to these elements in a manner that inspires confidence, related activities in the development and marketing of new products, services or legislation, such as privacy by design, privacy impact assessment and accountability will have to be prescribed, mandatorily or otherwise, in new legislation and regulations.

And finally, a relevant role has been reserved for the supervisor, the Dutch DPA – or rather the Dutch Data Authority - in order to promote compliance with the fundamental right to the protection of personal data, as laid down in the Lisbon Treaty. If the legislator fails to provide said Authority, by means of the upcoming legislative amendment, with the means to increase the chance of catching those who violate the law, fails to provide it with the power to issue fines, which power should have a deterrent effect and therefore be considerable, and fails to oblige it to report publicly on its findings, the chance is considerable that compliance with the fundamental right to protection of personal data becomes a fiction. A supervisor should have sharp teeth so that it needs to use them as little as possible!

Jacob Kohnstamm
Chairman

INTRODUCTION

The Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens, CBP] encourages compliance with the rules regarding the protection of personal data, if necessary by imposing enforcement measures. Without adequate protection of these data the fundamental right to protection of personal data cannot be fully asserted.
Due to the technological developments and rapid globalisation, citizens are hardly able to keep track of their data anymore, nor are they able to have a sound grasp on the processing of these data. That is why the Dutch DPA takes the view that controllers – organisations and governments – have to take action now. They should demonstrate that they collect and process the personal data of their customers and citizens in accordance with the law.

In its supervisory role, the Dutch DPA uses various approaches and tactics with the purpose to ensure compliance with the Dutch Data Protection Act [Wet Bescherming Persoonsgegevens, Wbp]. Some situations require an immediate response, as was the case when the CBP initiated talks with the mayors of Ede and Enschede about the registration of Roma in their towns. Other circumstances require more lengthy investigation, possibly followed by enforcement. For instance in 2010 the final stages of the investigation into hospitals' security measures regarding their patients' data were carried out. Following enforcement action concerning incremental penalty payments, the last of the hospitals which had been inspected executed a satisfactory new risk analysis and in doing so complied with security norms for the health sector. The investigation which was undertaken in 2009 into the collection of sensitive data of people who frequented a website and the subsequent selling of their profiles, was also finalised last year when the company made clear which reparatory measures it had taken.

Some other investigations that are mentioned in the annual report concern the processing of personal data of students and their use of a public transport pass, the linking of data files by the social security investigation service as well as the input of police files in the Europol Information System. Apart from these extensive investigations numerous other investigations and interventions on a smaller scale take place every year, often concerning (the removal of) personal data from the internet.

The Dutch DPA decides which cases it will investigate on the basis of risk analysis. In which sectors are citizens subjected to risks of serious and structural breaches of the Dutch Data Protection Act? In order to answer this question, the Dutch DPA uses the signals citizens lodge at the CBP via its two websites. The websites in turn provide the citizens with information in order to enable them to take action themselves if they believe their personal data are not being processed in accordance with the law.

Furthermore, the CBP advises the government on draft legislation, to ensure that already from the initial stages of the legislative process guarantees are provided for the protection of personal data. The Annual Report includes several examples concerning draft legislative proposals which have been amended following the advice of the CBP, with the aim to avoid a possible violation of data protection legislation.

Increasingly, processing of data has a cross-border nature. Problems which arise in the Netherlands concerning data protection also surface in other countries. Especially in the Article 29 Working Party, national Data Protection Authorities of EU-member states co-operate intensively, for instance to adopt a joint strategy with regard to the future of the EU legislative framework on privacy. Other examples of cooperation are the mutual recognition of the

assessment of Binding Corporate Rules and the undertaking of joint proceedings against influential parties as for instance Google. Last year more initiatives were undertaken for international co-operation, like the establishment of the Global Privacy Enforcement Network (GPEN).