Dutch Data Protection Authority - Annual Report 2014

Foreword

October 2015 holds some very exciting days in store for everyone close to the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)], because at the end of October the Dutch DPA will host the 37th International Privacy Conference (International Conference of Data Protection and Privacy Commissioners) in Amsterdam. About 800 leading privacy experts from different stakeholders in the private and public sectors, such as academia, representatives from non-governmental organisations as well as from data protection authorities, from around the world, will then discuss the current state of privacy.

This current state of play of privacy in the world is a topic that is more than worth discussing. The extent to which security services seem to be keeping tabs on the lives of everyone is worrying, but also the ongoing search for an effective way of monitoring and supervising the activities of these security services, have received great attention since the revelations made by Edward Snowden. The unprecedented, immense collection of personal data by large (mostly US-based) IT multinationals is another cause for concern.

Considering that national borders have become virtually non-existent due to the Internet and developments in IT, there is no doubt that the setting of social parameters governing the collection and processing of personal data has long since ceased to be merely a national issue.

For these reasons the European Union is currently working on a new legal framework on data protection in the European Union. The new legal framework will harmonise the rights and obligations applicable regarding the protection of personal data in all Member States. The new Regulation is based on the principle that the protection of personal data is a fundamental right. Therefore, personal data can only be collected and processed on the basis of a limited number of legal grounds, for example, when there is a legal obligation to do so, on the basis of the legitimate interests of the controller, or where the individual has explicitly provided his or her informed consent, amongst others.

In the United States, the issue of 'privacy' is regarded quite differently. The protection of personal data in the US is enshrined in consumer law: the collection and processing of personal data is permitted, unless when used for 'false or deceptive' practices, for example when it is used in violation of the general terms and conditions applicable to the product in question or the relevant service.

The differences in the manner in which the protection of personal data is enshrined in law on each side of the Atlantic Ocean are causing significant problems. Many new, useful and interesting products and services come from Silicon Valley and have extraordinarily successfully been introduced on the European market. However, as these products and services are generally paid for by 'merely' providing personal data, without the company having a legal ground in the EU to process the data, the processing operations are in flagrant violation of the applicable law in the EU. Citizens, governments and companies in the EU are consequently confronted with

devilish dilemmas, all the more so since the companies providing these products and services have market shares bordering on a monopoly.

Since in the EU a final decision will hopefully be taken soon about the new Regulation on data protection, but in the US the differences between the Republicans and the Democrats, also in the area of possible legislation on privacy, stand in the way of decision-making there, it is very likely that the trans-Atlantic differences on this issue will not be resolved anytime soon by new legislation.

Following the analysis above, the Massachusetts Institute of Technology (MIT) and the Institute for Information Law of the University of Amsterdam (IViR) have, much to our appreciation, brought together twenty privacy experts from both sides of the Atlantic to participate in the Privacy Bridges project. The aim of the project is to find a number of pragmatic, practical and/or technological solutions – or bridges – taking the differences in privacy legislation in the EU and the US as a given. These bridges should ultimately lead to a higher level of protection of personal data, while making the differences in the legal systems less burdensome on all concerned. It is moreover assumed that the 'privacy bridges' resulting from this project could also help in addressing differences in privacy legislation between the US, the EU and other parts of the world for citizens, companies and governments.

The results of this project will be presented and discussed at the end of October 2015 in Amsterdam during the 37th International Conference of Data Protection and Privacy Commissioners, where the focus is to be on 'Building Bridges'. The aim of MIT, IViR and the Dutch DPA is to have very concrete and direct actions as the result of the project and the conference.

The International Privacy Conference takes place on the eve of the Dutch Presidency of the EU (in the first half of 2016). It would of course be wonderful if a few of the formulated 'privacy bridges' were to be implemented during the EU Presidency of the Netherlands, in cooperation with the European Commission and the American government, paving the way for making life a little easier for all, but most and for all providing a higher level of personal data protection on a global level.

Jacob Kohnstamm
Chair of the Dutch DPA

Introduction

The Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] stands for the fundamental right to the protection of personal data. The Dutch DPA supervises processing of personal data in order to ensure compliance with the provisions of the law on personal data protection and advises on new legislation. Every year, the Dutch DPA identifies a number of topics which merit special attention. In 2014, the main topics were profiling, decentralisation and data processing with regard to employment.

Priorities are determined on the basis of information we receive from various sources in society and via different means. The Dutch DPA for example is actively following relevant technical and legal developments and remains in contact with different stakeholders, such as branch-, consumer- and human rights organisations. Questions and tips received about potential violations, of which received approximately 7.000 annually, are also important input for determining our priorities, as well as contact with the press and items covered in the media.

The Dutch DPA has in 2014 concentrated in its activities on the manner in which organisations inform people on the processing of their personal data and how they obtain consent , in so far as this is required by law. Due to the size and complexity of most data processing operations, people are often unaware of the nature and consequences following the (re)use of their personal data. It is therefore of utmost importance that organisations are transparent about this. One of the legal grounds for processing personal data is the informed consent of the individual concerned, but often consent is not obtained in a correct manner. The Dutch DPA has therefore conducted a number of investigations to determine if the conditions of valid consent were met.

In 2014, the Dutch DPA also paid special attention to the security of personal data and investigated whether organisations had put in place the necessary technological and organisational measures.

A selection of the activities carried out by the Dutch DPA in 2014 is provided below:

Profiling
The use of tracking cookies, which monitor the behaviour of Internet users across multiple websites, enables organisations to collect large amounts of personal data. By subsequently analysing and/or combining this data, organisations can label people according to specific categories (profiles) and treat them differently or approach them in a more targeted manner. While this can certainly be beneficial, for example when only personalised advertisements are shown, this should only be done when people have made a genuine choice, after having been properly informed.

The Dutch DPA has conducted an investigation into the advertisement company YD (now called Yieldr) and concluded that the company was violating the law by using tracking cookies to collect personal data of internet users with the aim of showing them personalised advertisements. Yieldr did not ask for consent, but only offered an opt-out, which is in violation of the law.

In another investigation, the Dutch DPA found the Nederlandse Publieke Omroep (NPO) [Dutch Public Broadcasters] to be in breach of the regulatory standards, since it was using tracking cookies to profile the surfing behaviour of visitors to the websites of several broadcasting stations, without seeking their prior consent. The Dutch DPA established, among other things,

that on all NPO websites analytical tracking cookies were already being placed at the moment a web page was loaded, so before giving the user the possibility to choose . The Dutch DPA also established that the information provided by the NPO to those visiting its website about the different kinds of cookies used and about what personal data would be used for which purpose(s), was incomplete, inconsistent and at some points factually incorrect.

In 2013, the Dutch DPA published its Report of Findings of the investigation into the amended privacy policy of Google. The investigation showed that Google appeared to be combining the personal data of Internet users for various purposes, including showing personalised advertisements. Google could combine information about, for example, conducted searches, location data, watched videos and e-mails with each other, while the different services had very different purposes. What is more, Google did this without informing Internet users properly and without asking them for consent. In 2014, the Dutch DPA issued an order against Google, to stop the violations of the law, subject to a penalty payment in case of non-compliance. The penalty could rise to 15 million euros.

Decentralisation
Since 1 January 2015, the municipalities of the Netherlands have new tasks in the area of youth care, work & income and care for the elderly and those suffering from long-term illnesses (also known as the 'social domain'). The preparations for this decentralisation - transfer of tasks - from central government and the provinces to the municipalities took place in 2014. Among other things, the Dutch DPA responded to the policy document of the Ministry of the Interior and Kingdom Relations regarding privacy in the social domain, in which was said that municipalities would be gaining experiences by 'learning by doing' and an evaluation would take place in due time. The Dutch DPA made clear that 'learning by doing' does not mean that municipalities would be allowed to suspend compliance with the Wet bescherming persoonsgegevens (Wbp) [Dutch Data protection act].

The Dutch DPA was also asked to assess the results of a privacy impact assessment for the so-called 'youth domain' (special care related to youth). The most important message from the Dutch DPA was that a proper, comprehensive legal basis for the processing of personal data for the performance of new tasks in various sections of the social domain is missing. Municipalities can choose from a variety of options to perform their new tasks, with different parties and processes. In this regard, they are required to establish on which legal ground they are basing their processing operations. The Dutch DPA recognizes that determining the correct legal basis can in practice be time-consuming, complex and sometimes even impossible. This is true not just for the youth domain but to the social domain as a whole. The Dutch DPA therefore urgently advised to the government to provide for a comprehensive legal basis.

Employment relationship
Randstad and Adecco, two of the biggest employment agencies in the Netherlands, were found to be in non-compliance with the law on various points when processing personal data of temporary agency workers, an investigation of the Dutch DPA showed. Both employment agencies for example asked temporary agency workers who called in sick about the nature and cause of their illness and filed this in their systems. In addition, Randstad and Adecco both made copies of people's identification documents during the intake interview, which is not allowed yet at that stage. Adecco moreover in contravention of the law provided copies of these identity documents to its clients. Finally, the investigations also showed that the personal data of

temporary agency workers was being retained by Randstad and Adecco for longer than was necessary.

The Dutch DPA investigated the security of the Suwinet system, which enables various government organisations to exchange (sensitive) personal data related to work and income. It is very important that the data is kept secure and is accessible only by duly authorised members of staff. The security measures put in place were found to be inadequate both at the UWV [the body in the Netherlands that implements employee insurance schemes] (the Suwinet system's administrator) and at the Municipality of Den Bosch (a client). Many of the required plans or procedures were not up-to-date, were incomplete or unfinished. Both the UWV and the Municipality of Den Bosch had failed to adapt their security plan specifically related to the Suwinet system. Moreover, security incidents were not centrally analysed and handled.

Cross-border cooperation
The Dutch DPA participates in different European cooperation platforms, such as the Article 29 Working Party and the supervisory bodies regarding, amongst others, Europol and Eurojust. In these fora, the Dutch DPA focused in 2014 on topics such as big data and surveillance by the security services. As in 2013, the Dutch DPA spent much time on the revision of the European legal framework on data protection currently ongoing. In addition, the Privacy Bridges project was launched in 2014 at the initiative of the chairman of the Dutch DPA. The project consists of 20 American and European privacy experts, who are looking for practical solutions for bridging the transatlantic differences in legal systems regarding the right to personal data protection.

The Dutch DPA's working procedure

The Dutch DPA is the authority in the Netherlands charged with supervising compliance with the Dutch Data protection act and related legislation. In order to promote compliance, the Dutch DPA deploys a variety of instruments in the area of supervision, enforcement and communication.

Supervision
The Dutch DPA is not in a position to investigate every alleged violation of the law. It has therefore developed a set of criteria to determine whether or not to conduct an investigation. The Dutch DPA will conduct an investigation when there is a suspicion of serious and structural violations that affect a lot of people, that can be addressed by using its competences and if the issue at stake falls within the priorities it sets annually.

The Dutch DPA may also choose, for example, to send a warning letter to an organisation or to speak with it on the matter at hand. This will mainly be done with regard to possible violations that do not meet the criteria mentioned above. Such a letter or conversation may already be enough to bring the violation to an end. If an organisation refuses to cooperate or if the Dutch DPA receives further complaints against this organisation, it may decide to investigate.

Enforcement
When the Dutch DPA has, in an investigation, established violations that are still continuing, it can start enforcement action. The Dutch DPA is competent to impose a conditional fine on organisations, subject to a penalty for non-compliance. They will be given a certain period to terminate the violations. When the organisation fails to do so, it will have to pay the financial penalty set, which can amount up to a given maximum.

Communications
External communication is also an important instrument in reaching compliance with the law. The Dutch DPA maintains contact with the media, it meets with branch organisations and other stakeholders and gives presentations on a regular basis. In addition, the Dutch DPA provides information by telephone via the hotline which can be reached every day and on its website (completely revamped in 2014): Cbpweb.nl.