

## **EC Conference Directive 95/46/EC**

### **Workshop 1: For a better implementation of the Directive.**

Chairperson: Mrs Elisabeth France

Rapporteur: Mrs Rosa Julià Barcelo

Speaker: Prof. dr. Michel Walrave, University of Leuven - Belgium

Brussels, 30 september 2002

To try to give some suggestions for a better implementation of the directive, we can start by observing the actual situation, namely the implementation of data protection legal obligations in our countries in several domains where personal data are processed.

One of the data-intensive economic areas is direct marketing in general and internet marketing in particular. By observing the way in which data are processed, we can formulate our comment or advise. Because, based on the weaknesses of some privacy policies that we can point at, we can discover which aspects of the directive are not or not enough followed and maybe not understood by organisations. But also based on the strengths of some privacy policies we can draft best practices.

This is the reason why I would like to share with you some general trends of the research I have done in Belgium about data protection in websites. I have measured in commercial business-to-consumer websites, the implementation of the directive transposed in the Belgian privacy law.

Based on the results of this scanning of 250 websites that collect personal data, I will point at some weaknesses of actual online privacy protection and how data protection may be better implemented. This analysis was first done in 2001 before the new Belgian privacy law came into effect, conforming the Belgian law to the European directive. A second analysis of the sample was done one year later, to observe possible changes.

I will browse with you through a few trends I have observed that inspired my recommendation.

In 2001, 43% of the businesses represented in Belgium and collecting personal data online posted a privacy statement on their website, this increased to 55% one year later. On first sight this could be seen as a positive trend, but let's not forget that today still 45% of the analysed websites that collect personal data offer no legally obliged information. Moreover a majority of the online privacy statements are not completely in conformity with the legal obligations. When we have a closer look at those privacy statements we see actually that:

1. The information about the responsible for the data processing is not **complete**, purposes of the data processing are sometimes vague and not all privacy rights, namely right to access, rectify and to object are explained in the online privacy pledge.
2. When the rights are explained, they omit often easy to use **procedures** to exercise those rights. For example, a minority offers a secured online access to own personal data to correct mistakes. Also a minority offers an online right to object against the processing of personal data for direct marketing purposes, using a tick box.
3. A majority of sites are not only collecting data in an explicit manner, using one or several electronic forms, but in an **implicit** manner as well (using cookies or other software to track the click stream of the website visitor). We have focused on the use of cookies by the website responsible and possible third parties. The result is that only a small percentage (namely 12%) inform their visitors about the reason why they use cookies.
4. Next observation concerns the comparison between the purposes of the online data processing expressed in the privacy statement and the number and type of data that are collected. There is actually often an **imbalance** between purposes that are communicated and the data collected. Half of the online forms indicate the difference

between necessary data to attain the explicitly mentioned goals, and the data that are optional.

5. Finally, we tried to have access to the internal **implementation** of the privacy promise. We have sent an e-mail to the responsible for the data processing, asking a simple question about the privacy policy of the company. Less than half of the companies answered to this e-mail. From the answers we received, two thirds were to the point. This could mean that some companies making a privacy promise on their website, do not communicate this information internally to persons who have to answer e-mails from website visitors. This could mean also that some 'privacy promises' are a kind of 'copy paste privacy statement', electronic window dressing to stimulate trust of website visitors, to be quickly in accordance to some legal obligations, without integrating the privacy promise in the organisation's policy.

These are a few trends we have observed during our analysis of online privacy statements. Our conclusion is that for a better implementation of the directive, we need **segmented information campaigns that translate the principles of the data protection directive into concrete practices of different sectors**, to make the rights of the data subjects more tangible. On the one hand, consumers have to be informed about their privacy rights but also how they can demand the exercise of these rights backed by their national Privacy Commission.

On the other hand, businesses have to be offered a translation of the privacy principles into concrete do's and don'ts to make the implementation of the privacy rights easier to integrate in their day to day practice. Furthermore, we have observed thresholds that make the exercise of privacy rights difficult for consumers. So, organisations need not only to know what promise they have to make, but also how they have to organize easy to use procedures to be able to keep that promise. That's why examples of **specific procedures** can be proposed in codes of

conduct or made compulsory by other means to augment the effective enforcement of the privacy rights.

Conclusion:

Finally, responsables for data processing not only have to be informed, but also their sensitiveness for privacy concerns of consumers has to be increased. Because those privacy concerns have implications not only for the trust consumers have in new forms of interactive communication and marketing, but also influence the quality of the databases that businesses are building. We conclude this, based on our survey among internet users. More than 60% admit to have communicated false data, when they doubted the necessity of this information for the purpose that was communicated.

A lack of trust and control over own personal data can lead to weak database quality and maybe to less opportune communication. So protecting privacy of individuals who are entrusting their personal information is not only an important token of respect for that person, is not only the implementation of a legal obligation, but it is also a necessity to contribute to the good functioning of interactive communication between companies and consumers. Businesses cannot build long-term loyal relationships with consumers by analysing only their needs and wishes concerning their products and services. They have also to be all ears for the wishes and remarks consumers have about the use of their personal data and furthermore if and how they can communicate with them individually.

Prof. dr. Michel Walrave

K.U.Leuven - Departement of Communication Science

Van Evenstraat 2A, B-3000 Leuven, Belgium

+ 32 (0)16 32 32 29

Michel.Walrave@soc.kuleuven.ac.be