153, Gistelsteenweg
8490 Varsenare
Belgium
www.leewhiteconsultants.com

Summary report on the compliance of Belgian websites with regard to the processing of personal data in accordance with the Belgian Law on Privacy Protection in relation to the Processing of Personal Data, implementing European Union Directive 95/46/EC

Irina Nock Krishnan
LLB (Hons) London
LLM in Computer & Communications Law (Lon)
CLP (Malaysia)

Jos Wittevrongel
Microsoft Certified Application Developer (MCAD)
Microsoft Certified Professional (MCP)

Lee & White Consultants

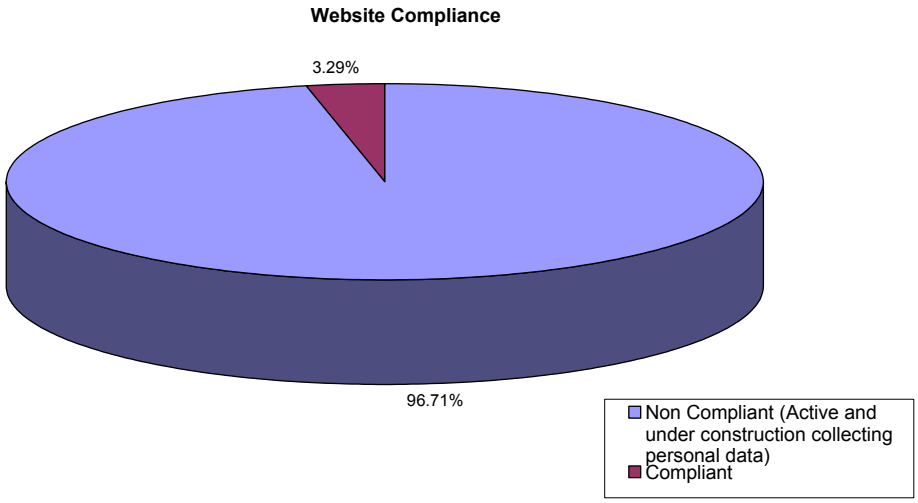
The advent of the Internet has led to many apparent advantages of having a presence in this global system. Businesses and organisations are setting up websites to mark their place on the Internet. A recent study assigned by the Federation of Belgian Enterprises in 2002 demonstrated that approximately 80% of all Belgian companies had a website, and about 27% of all Belgian companies have integrated Internet in their business activities and can be considered "e-visionary" companies. Undeniably, e-commerce websites and websites simply providing information about a company's products and/or services are an integral part of conducting business today. Yet, in the pursuit for global business recognition, legal conformity is a small price to pay. This legal conformity is in relation to the EU Data Protection Directive and the Belgian law on Privacy Protection in relation to the Processing of Personal Data.

Privacy is the core of the business and customer relationship. A company's attitude towards upholding an individual's privacy (both online and offline) will ascertain its success or failure in building a relationship with its customers, gaining their trust and developing that essential viable edge in the marketplace.

To that extent, Lee & White Consultants has produced its first report in a series of studies on the legality of Belgian websites in terms of complying with these privacy legislations and protecting Internet users' personal data - be it the regular surfer, potential customer(s) or existing customers. The numbers obtained reveal some extremely poor results for compliance with the Data Protection Law in Belgium. Evaluation of these websites from September 2004 - June 2005 confirms that Belgian websites are doing little to comply with the EU Data Protection Directive and the Belgian law on Privacy Protection in relation to the Processing of Personal Data in terms of having an adequate privacy statement on the website.

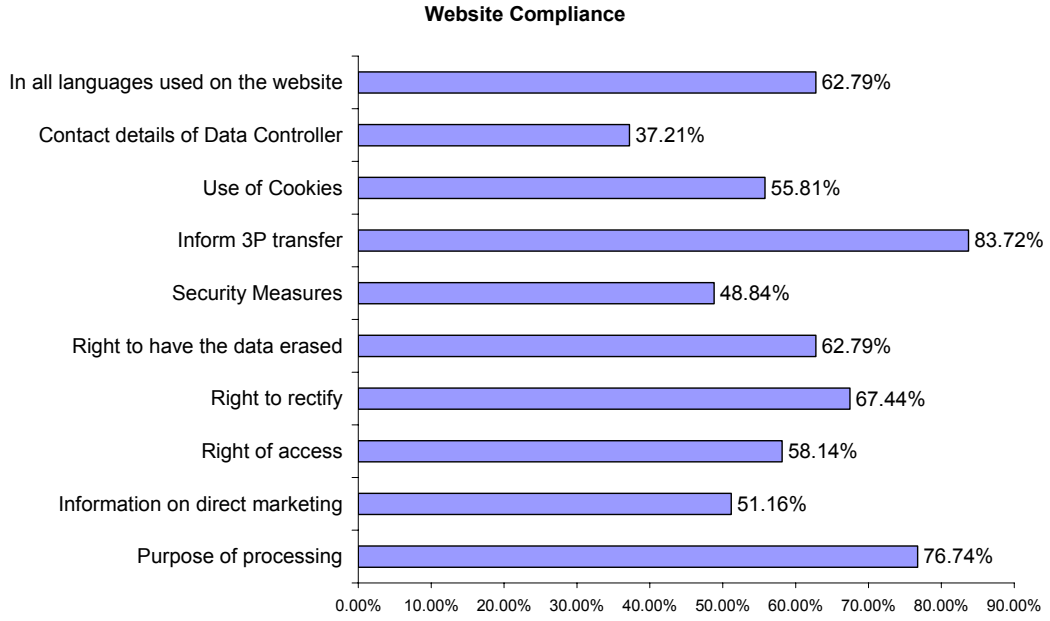
Thirteen years and several modifications down the road show hardly any progress has been made since the enactment of the Belgian law of 8 December 1992 to actively comply with the legal obligations stipulated.

Out of the 350 companies chosen, 220 companies had a virtual presence via a website. Out of these 220 websites evaluated, 213 were positively processing personal data. Out of the 213 websites processing personal data, 96.71% failed to comply with the law.



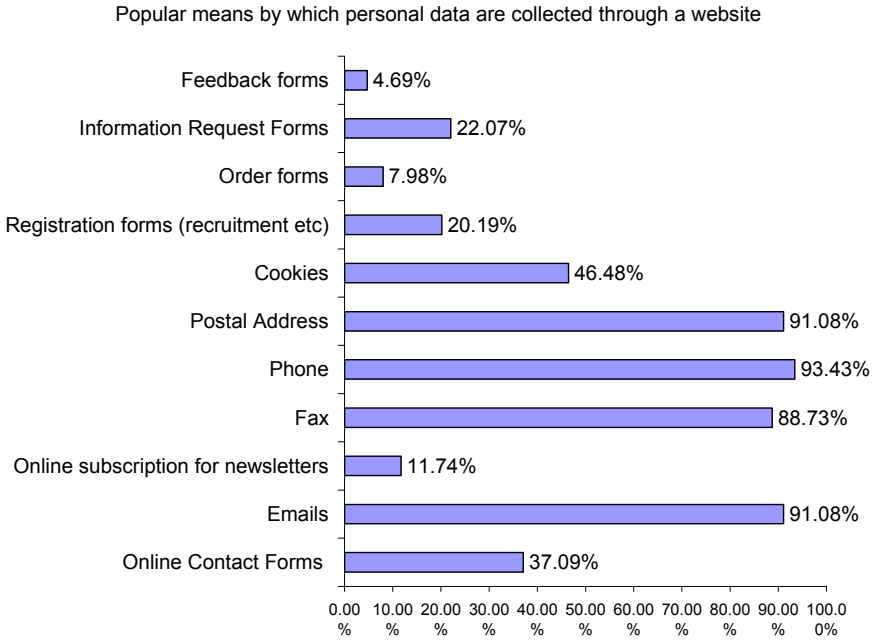
These websites were non-compliant in terms of either having a very inadequate form of privacy statement (16.90%) or having no privacy statement whatsoever (79.81%). The chart below illustrates that despite having a privacy statement, most websites do not include all the necessary

information and procedures for the Internet user – the most fundamental and glaring shortcoming being the absence of one of the most simplest requirements to follow - the contact details of the data controller.



Also with the recent Belgian Law in relation to Electronic Communications of 13 June 2005, the *strict* interpretation of Article 129 requiring information concerning the use of cookies on websites to be given *prior to the processing* might just mean that none of the websites researched are actually compliant with the Belgian Law in relation to Electronic Communications of 13 June 2005 although at the time of research, 23% of those which use cookies seem to mention the use. The reason for this is that those websites which do mention the cookie use do so in a legal disclaimer or privacy statement which is tucked away within the pages of the website and not available from the outset. This means that the cookies have begun operation prior to the information being given. However, this will be dealt with in a future report as this research was completed prior to the enactment of the Belgian Law in relation to Electronic Communications of 13 June 2005.

The following popular ways of collecting personal data through a website were also observed:



Online forms including subscription for newsletters seem to make up the most common method of processing personal data on a website but it was noted that in many cases, the information requested for does not correspond with the purpose of processing – contrary to the requirement under Article 4§1 of the Belgian Data Protection Law that the processing of personal data must be for specified, explicit and legitimate purposes and not excessive in relation to those purposes. The obligatory or optional nature of the information to be provided must be clearly stated.

However, the analysis revealed that only 53.96% of the websites with online forms marked the obligatory information as mandatory whilst 46.04% of the websites did not do so. Moreover, 16% of the websites which did mark their fields as mandatory used the user's choice not to provide optional information against them by displaying error messages that the particular fields were not entered and thus prevent the user from being able to submit the form. As for those websites which did not mark their fields as mandatory from the outset, 32.81% used the user's choice not to fill in some of the fields against them contrary to legal obligations.

A one-to-one dialog held with a selection of the evaluated companies as a spot check revealed the general attitude of the non-compliant companies towards their illegality and how they use the low risk of being caught as an excuse not to rectify their problem. Since the illegality of only a minute number of companies has been exposed and to that extent, at an underrated scale, it waters down the urgency, importance and necessity for the protection of personal data.

At the same time, many companies through trial and error seek to formulate a reasonable version of a privacy statement and have it up on their websites rather than get professional assistance on the basis of saving cost. This is based on a misassumption that they are cheaper off doing it themselves without proper assistance. Research showed that some of the companies that were informed of their non-compliance later on put up privacy statements which were incomplete. Although it is commendable that these companies are trying to adhere to the laws, it is perhaps better to get it right the first time.

It would seem then that the low risk of being caught factor is linked closely to the cost factor. Companies believe that there is too much work to be done and fear the costs of hiring legal experts are too high for such a small risk of being caught. This is certainly not the case, as the overall cost for putting themselves right certainly outweighs the cost incurred from the possible legal sanctions such as:

- fines up to 500,000€
- publication of judgment
- confiscation and destruction of carriers of personal data
- cease and desist processing personal data up to 2 years
- possibility of imprisonment for repeated offences under the Belgian Data Protection Law

More so, the cost factor is surely outweighed by the success of building a trust relationship with customers which undoubtedly gives a competitive edge in the business world.

It also shows that these companies are mistakenly hiding behind their web design subcontractors rather than accepting their responsibilities on internal data processing and processes.

Companies also argued that there is no pressing need to specifically inform the data subjects the details of processing since businesses are normally conducted in an informal manner and reciprocal good faith between customers and suppliers is practiced. Without legal pressure from customers to ensure compliance, companies do not want to waste time on this area.

It is high time to educate users and consumers on their privacy rights and the privacy risks involved upon embarking on the Internet and of the avenues for complaints and redress. Simultaneously, organisations should be taught of their duties and the risks involved in the event of non-compliance. Just as the act of not paying company tax amounts to an illegal conduct, so too is the case of non-compliance with the privacy laws.

One good way of instilling a realisation of the importance of complying with their duties under the Belgian Data Protection Law is to make data controllers see themselves as data subjects. As a data subject, privacy is of the utmost importance. As such, to ensure others protect your personal data, you must first set the precedent yourself.

In fact, a joint initiative between government and private sector aimed at helping consumers and businesses towards protecting privacy is a good campaign to enhance legal compliance.

The Privacy Commission should also actively reprimand and fine companies in breach of the Belgian Data Protection Law. By applying enforcement and sanctions, there may be hope for discouraging non-compliance with the law and encouraging those who effectively comply to continue doing so.

For the full version of this report, please contact Lee & White Consultants bvba after reading our privacy policy available at www.leewhiteconsultants.com