# P3P Compliant Privacy Policies and European Data Protection Legislation

Jos Dumortier
University of Leuven (Belgium)

Social research has demonstrated that basic privacy principles are not very well respected by commercial website owners when they process personal data of consumers. Paradoxically compliance in this area is not substantially better in Europe – where we have comprehensive and rather strict data protection legislation – than in the US.

As a result of these statistical findings, consumer protection organisations in the US conclude that self-regulation is not sufficiently effective in this field and request the introduction of federal data protection legislation. In Europe similar statistical findings are increasing the scepticism about the ability of the law as an effective and sufficient instrument for regulation with regard to privacy protection of consumers on the Internet. This explains the recent European interest for standardization in this area.

There seems to be a broad agreement on the need for some set of recognized practices and procedures in this area. The regulators want to see mechanisms producing effectiveness and accountability. Businesses want to embed compliance into existing business practices using existing standardized mechanisms. They resist against a special set of measures for privacy and data protection that is not embedded in normal business controls. Business seems to look primarily for a solution removing uncertainty, scaleable to be widely applicable in order to minimize cost. Data subjects on their side want to see mechanisms inspiring confidence, substance and an element of independence assurance. For all these reasons there is a strong need to develop standardized rules and procedures in this area.

Standardization is a particular form of self-regulation. Like other self-regulatory mechanisms it is based on consensus and the resulting products – rules, guides, specifications and other tools – are essentially voluntary. They cannot be legally enforced unless they are incorporated in a legal instrument. The difference between standards and other forms of self-regulation is that standards are being produced in the framework of a recognized – not necessarily by governmental entities but primarily by market players - standardization body. Standards, in this sense, have certain benefits in comparison with other self-regulatory mechanisms.

P3P is a good example of standardization in the domain of consumer privacy protection. Its objective is not to provide an ultimate overall solution in this area but to give network users a tool for evaluating more efficiently website privacy policies and consequently to adapt their behaviour. Whether or not a particular privacy policy is compliant with the law is not a question that P3P can give a useful answer to. Privacy laws differ from country to country, even between Member States of the European Union where this matter has been harmonised by the Directive of 1995. A P3P compliant privacy policy is therefore not necessarily a privacy policy that is compliant with the laws of the website owner and of the consumer. It is even an illusion to think that such a degree of compliance can ever be reached, at least as long as privacy laws, especially in Europe, don't stay with generally recognized principles in this area. This can best be demonstrated with the example of what the European directive calls "special personal data". According to the laws of some of the EU Member States, processing this category of data is sometimes prohibited even when the controller of the data has received the explicit permission of the data subject.

Some privacy advocates in Europe are therefore criticizing initiatives such as P3P with the argument that privacy rights are not negotiable because they belong to the fundamental rights of the citizens. A fundamental right can inherently never be the object of a contract between the website owner and a consumer.

This problem should be solved sooner or later. To improve the usefulness of tools such as P3P we need a set of generally accepted data protection principles for the Internet. The current legal situation makes it impossible for owners of globally oriented websites to be compliant with the details of the all data protection laws issued in the countries of potential consumers.

For the time being we have to live with a pragmatic solution. As far as the European Union is concerned, privacy policies of website owners established outside the US, should be compliant with a set of minimum data protection principles. These principles have been formulated in a recommendation of the Working Party of the European data protection commissioners in 2001 (see further http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp43en.pdf).