Data Protection Online: Alternative Approaches to Sensitive Data?*

Rebecca Wong
Law Department, University of Sheffield

Abstract
The paper aims to review the criterion of "sensitive data" under Art. 8 of the Data Protection Directive 95/46/EC (DPD) in the online environment. Sensitive data is defined under Art. 8 as 'personal data revealing racial origin, political opinions or religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life.' Following the Lindqvist case (C-101-01), it is questionable how the criterion applies in practice. More specifically, it can be contended that any images/photographs of the data subject uploaded on the internet falls within Art. 8 of the DPD because the image/picture reveals some of the characteristics that may be regarded as sensitive data. The paper also takes account of Professor Simitis's report entitled Revisiting sensitive data published in 1999, which examined whether "sensitivity" really was a valid criterion for determining the conditions of the processing in the context of the Council of Europe Convention on Personal Data. In this review, the paper calls for a change in how sensitive data is assessed. It considers the purpose-based and contextualised approach to sensitive personal data in the online environment.

Keyword: Sensitive data, data protection, online

I. INTRODUCTION

The paper examines the concept of "sensitive data" as defined under the Data Protection Directive 95/46/EC (DPD) (hereinafter termed "DPD") and considers whether the categorisation of sensitive data should be amended in the light of technological developments. Under Art. 8(1) of the DPD, sensitive data is defined as 'personal data revealing racial origin, political opinions or religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life.'

However, when Art. 8(1) of the DPD is applied on the internet, it is questionable whether the criterion works in practice. More specifically, the case of Lindqvist (C-101/01)[1] demonstrates the problem of publishing personal information containing sensitive data on the World Wide Web. In this case, L had uploaded a web page containing details about members of a Parish Church. The website also included information about a member who had injured her foot. When the case was referred to the European Court of Justice (ECJ) for a preliminary ruling, the issue was whether the publication of a member who had injured her foot constituted the processing of "sensitive data" because this was data concerning the health of an individual. Leaving aside the exemptions under Art. 8(2) of the DPD, my main concern is the broad application of Art. 8 DPD to anything published on the web page, which directly or indirectly refers to anyone having a political opinion, religious or philosophical beliefs, trade union member or data concerning the health or sex life. Another area of because the processing of personal data revealing racial origin? To put it another way, if I had published a picture of an Eskimo, would I be processing sensitive data because the picture reveals the Eskimo's racial origin? Under the DPD, Art. 8(1) would apply irrespective of how trivial the case may be.

These are questions that are not easy to answer, but the paper will firstly consider the origins of sensitive data. This will be followed by the current approach adopted under the DPD and the Lindqvist[2] case. I will then look at Professor Simitis's report (1999) entitled Revisiting sensitive data and consider the arguments in the light of the online environment. By online environment, I am excluding manual files containing personal data such as card indexes. I am referring specifically to the internet and the World Wide Web.

---

* A version of this paper was published in Complex 4/06 - Sylvia M. Kierkegaard (ed.): Legal, privacy and security issues in information technology

[1] 2004] 1 C.M.L.R. 20

[2] *Ibid.*

2. ORIGINS OF SENSITIVE DATA

Sensitive data was originally introduced under the Council of Europe Convention 1981 on Personal Data (hereinafter termed "CoE Convention"). Art. 6 of the CoE[3] Convention provides that

> Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

The CoE 1981 and the OECD Guidelines on Personal Data 1980 (the latter is not discussed here) have been influential in the developments leading up to the DPD. Furthermore, these international instruments have been a model to some countries enacting data protection laws (Bygrave, 2003).

According to Simitis (1999), the categorisation was readily accepted without question within the DPD. Although member states of the European Economic Area have implemented the DPD including Art. 8(1)4 on sensitive data, the question that has arisen is whether the categorisation falls short of the dangers highlighted in recent technological developments? To give an example, the Council of Europe report (entitled Informational self-determination in the internet era) recommended that identification numbers that enable many databases or data to be connected together should be included within the definition of "sensitive data". This practice has become widespread in the public and private sector. The DPD however, leaves it to the discretion of the member state to determine the conditions under which a national identification number or any other identifier of general application may be processed (Art. 8(7) DPD), but does not specifically touch on the subject of identification numbers in the online environment or its use in databases.

Secondly, the category should also cover "profiling". This is defined in Swiss law as 'a combination of data that enable an aspect of the key aspects of the personality of an individual to be made.' (CoE Report, 2005). The report suggested that anonymous profiling should be included when this is used to take subsequent decisions concerning persons covered under this profile. It is interesting to note from the report that the current definition of sensitive data is too wide and we should abandon the approach based on the definition of the actual nature of data in favour of a purpose-based approach. To put it another way, what is the purpose of such processing? Is the processing intended to reveal sensitive data such as political opinions? This alternative would not only be pragmatic, but also resolve the difficulties highlighted in Lindqvist,5 where any personal information published on the web could theoretically fall within Art. 8(1) involving the processing of sensitive data. This is a slightly different from the contextualised approach that I will be exploring later. What I mean by contextualised approach is that personal data becomes sensitive according to its context as argued by Simitis (1999). Before examining both approaches, I want to examine the case of Lindqvist6 in the next section looking at the implications of the European Court of Justice's decision.

3. THE IMPLICATIONS OF LINDQVIST

I have already discussed the facts of the *Lindqvist* case above and do not want to reiterate this here, so I want to consider the main issues under this case. The European Court of Justice (hereinafter "ECJ") had to decide:

> Whether the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46?

---

[3] http://conventions.coe.int/treaty/en/Treaties/Html/108.htm, Last retrieved 20 February 2006.
[4] See PRIVIREAL. Data protection: countries (http://www.privireal.org/content/dp/countries.php), Retrieved February 2006.
[5] See n. 1.
[6] *Ibid.*

If the answer to the first question is in the affirmative, was the processing of personal data such as that described in the first question covered by one of the exceptions in Article 3(2) of Directive 95/46?

Whether reference to the fact that an individual had injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46?

Finally, the question is whether any transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person (the hosting provider) who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country? The referring court also asks whether the reply to that question would be the same if no one from the third country had in fact accessed the data or if the server where the page was stored was physically in a third country.

For the purpose of this paper, the relevant issue is the ECJ's decision to question three. In reply to the third question, the ECJ held that in the light of the purpose of the Data Protection Directive 95/46/EC, the expression "data concerning health" used in Article 8(1) thereof must be given a **wide interpretation** so as to include information concerning all aspects, both physical and mental, of the health of an individual (emphasis added). Therefore, reference to the fact that an individual has injured her foot and is on half-time on medical grounds constituted personal data concerning health within the meaning of Article 8(1) of Directive 95/46.

The court's wide interpretation of Art. 8(1) should come as no surprise for academics and practitioners engaged in this area of work. However, I was slightly puzzled and even amazed that the decision should come as a shock or even disbelief by some individuals including Lindqvist herself for the court's wide approach. My main objection was not the court's wide approach to the interpretation of Art. 8(1). Otherwise, it would, in my view, defeat the very objectives laid down under Art. 1(1) of the DPD. Art. 1(1) protects the fundamental rights and freedoms of individuals including privacy. Rather, my concern was grounded by the fact that the original legislators (to the DPD) felt it necessary to have a category on sensitive data, meriting further protection. Why give preference to this particular category?

The publication of personal information on the web (whether by individuals or organisations) also underlines certain dilemmas for data protection authorities that oversee and enforce the data protection laws within their own member state.

Should the data protection authorities adopt a literal approach to their own data protection laws by requiring that individuals obtain consent before he/she publishes personal data on the web? Or should the data protection authorities adopt a flexible or teleological stance so that individuals (whether jointly or not) who intentionally publish personal data on the World Wide Web with the aim of psychologically harming others are prosecuted? Some authorities such as the CNIL (French data protection authority) have published guidelines about the publication of health information on the internet. These guidelines do not apply in all the member state countries and therefore, divergences between these countries still remain. An added impediment is the prosecution of individuals by data protection authorities outside the EEA who publish personal data on the web. I am referring to countries that do not have data protection laws. How do data protection authorities enforce their laws outside their own country? (Korff, 2001). Art. 28 of the DPD expressly refers to the role of the supervisory authority and the working party on the protection of individuals with regard to the processing of personal data. The relevant provisions are Art. 28(1) and (6) of the DPD. Art. 28(1) states that:

> Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

Art. 28(6) further provides that:

> Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.
> **The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information** (emphasis added)**.**

Although these provisions give the added assurance of co-operation between supervisory authorities of Member States, it is not entirely clear how third countries (outside the EEA) as defined under Art. 25 and 26 applies. In other words, if an individual from a "third country" misuses personal information of an individual in an EEA state, it is questionable whether the individual can seek redress from the offender without the co-operation of the supervisory authority in the third country (assuming that the third country has a data protection authority). The picture is not completely negative because some countries such as Switzerland and Hungary have enacted data protection laws (that are modelled on the DPD) and the Commission has ruled that their laws have satisfied the "adequacy" requirements under Art. 25. Countries such as India and China, however, still fall short of the necessary requirements of "adequacy" (Privacy Exchange, 2006 and Privacy International, 2004 respectively). The issues that I refer to above are only the tip of the iceberg. Enforcement is not a topic I have dealt with in any great detail. It, however, serves to highlight the global nature of the internet/world wide web and the naive attitude adopted by original legislators to the DPD that enforcement can be taken at a national level without the willing co-operation of authorities from countries outside the EEA (including the US).

In the next section, I want to consider the different approaches to sensitive data and decide why the current categorisation (under Art. 8 DPD) based on the definition of the actual nature of data appears impractical and arguably antiquated with the general processing of personal data on the internet.

4. So which approach is it? A purpose-based or a contextualised approach?

4.1 Purpose-based approach

I should state from the outset that it was the Council of Europe Report into informational determination (2005) that originally put forward the concept of a purpose-based approach. I raise this subject because it is markedly different from the contextualised approach (considered below). In this section, I want to explore the main arguments to a purpose-based approach. As discussed earlier, a purpose-based approach looks at the purpose underlying the processing of personal data. Is the processing intended to reveal sensitive data? The approach has the advantage of targeting perpetrators or would be offenders who intentionally reveal data of a sensitive nature (as defined under Art. 8(1) and does not adopt a blanket approach to the application of Art. 8(1) DPD. Namely, that all personal data involving political opinions, religious beliefs of individuals (and so forth) would fall under Art. 8(1). Such an approach also (in my view) reduces the number of trivial cases (the principle of *de minimis non curat lex)* being brought before the court. In my view, it is also arguable that the administrative burdens placed upon data protection authorities would be lessened if this approach were adopted. In short, the main advantages are:

- Cost effectiveness – reducing the administrative burdens of data protection authorities.
- Teleological/purposive approach - directing Art. 8(1) DPD to the root of the problem.
- Observing the *de minimis* principle - the court should not be concerned with trivial cases.

- The question that remains to be answered is who decides whether the data in question is sensitive? Should one adopt an objective approach, so that a reasonable man in the shoes of the data subject would consider that the publication of personal data on the internet was sensitive and intended to harm him or her?
- If the purpose-based approach is to be considered seriously then the questions that I raise should be fully addressed so that there are no uncertainties (or at least minimised).

4.2 Contextualised-approach

A contextualised approach to sensitive data means that personal data becomes sensitive according to its context (Simitis, 1999). This was the approach adopted by Germany (Simitis, 1999). The German data protection laws (Federal Data Protection Act 2001 and Länder data protection laws) have, however, implemented the DPD to include the category of sensitive data. However, a contextualised approach takes an inclusive stance by refusing to adopt the current line of thinking under the DPD that certain categories such as religious beliefs, political opinions merit further protection. This is not to say that the processing of personal data revealing religious beliefs should not be regarded as the processing of sensitive data, but rather data may, under certain contexts/circumstances be treated as the processing of sensitive data.

In this section I want to consider the main arguments discussed by Simitis in his report back in 1999. The report arose from a review of the answers to the questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. It is interesting to note that differences existed in the interpretation of sensitive data between member state countries to the European Union before the DPD was implemented.

Countries, like Austria and Germany, that had consistently rejected all abstract categorisations of personal data and instead focussed on a **context-orientated appreciation** of the data, must consequently abandon their long-standing practice and for the first-time expressly recognise the existence of sensitive data (emphasis added).

The enumeration of sensitive data under Art. 8(1) (be it personal data revealing political opinions, religious beliefs and so forth), however leaves open the question about whether this list is exhaustive. Indeed, Simitis (1999) considered at the time that no specific category existed for genetic data within Art. 8(1). However, according to Recommendation R (97) 5 on the Protection of Medical Data, genetic data has been subsumed in the health or medical data (Simitis, 1999). Austria, Iceland, Norway, Portugal and Switzerland have also taken the view that genetic data fell within health or medical data under Art. 8(1) (Simitis, 1999). The issue of genetic data raises the debate about how extensive should the list for sensitive data be? More specifically, Art. 8(1) DPD is silent on "profiling" (Bygrave, 2002) and whether this type of activity justifies extensive protection because of the sensitive nature involved (whether it reveals political opinions, religious beliefs, health, trade union membership etc. is another matter) and the consequences arising from its misuse. It should be noted that "profiling" could be regarded as a "processing" activity within Art. 2(b) DPD. Art. 2(b) states that

'Processing of personal data' ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Profiling could include some of activities alluded above including the collection, storage, adaptation, alteration and the retrieval of personal data.

The contextualised approach (also termed as "context-orientated") is aptly summarised by Simitis (1999) as follows:

Sensitivity is no more perceived as an a priori given attribute. On the contrary, any personal datum can, depending on the ***purpose or the circumstances of the processing be sensitive****. All data must consequently be assessed against the background of the context that determines their use. The specific interests of the controller as well as of the potential recipients of the data, the aims for which the data are collected, the conditions of the processing and its possible consequences for the persons are factors that, put together, allow both the range and effects of the processing to be discerned and thus to determine its degree of sensitivity. An evaluation of the sensitivity requires hence more than a mere look at the data.*

In the context of the online environment, the current approach based on the actual definition of personal data is not satisfactory, because it simply adopts the line that the publication of personal information involving

political opinions, religious beliefs etc. falls within Art. 8(1). Leaving aside the exemptions under Art. 8(2), it neither questions why the processing is taking place nor considers the circumstances in which particular areas of processing be regarded as sensitive. For example, I raise a particular problem that has not been adequately addressed by the DPD. Would I be processing sensitive data simply by gathering information about an individual (with or without the data subject's knowledge), which reveals data containing religious views etc.? Under Art. 8(1) of the DPD, it would. However, in gathering the information, I form an opinion or an assumption that a person belongs to a specific religious group or holds a political opinion? To give a pertinent example, company X holds information about Y's reading habits. On the basis of this information, company X decides to send details about books that match Y's reading habits. What if Y's interest in the particular genre of books is only incidental? In other words, Y's company had made an assumption that X was interested in these particular books without ascertaining directly what Y's interests were. Unless Y verifies the information with X, then Y will continue to operate under this false "assumption". Is there some legitimacy in my argument or does it sound far-fetched? I raise these questions, because there are some companies that form a profile of an individual without verifying this information with the individual concerned (Bygrave, 2003). Indeed, Bygrave (2003) has extensively dealt with the subject of profiling in his book entitled Data protection law: approaching its rationale, logic and limits. To give a foretaste of this subject, he defines profiling as follows:

The profiling process has two main components: (1) the process of inferring a profile (2) the process of treating persons/entities in light of this profile.

I do not want to discuss profiling in any great detail because the paper is principally concerned with the current interpretation of Art. 8 on sensitive data. The point that the paper is leading to is that the current interpretation of "sensitive data" under the DPD should be reviewed or re-examined in the light of technological developments. Whether this would mean either adopting a purposive based or a contextualised approach towards sensitive data, it is a progressive step towards the right direction in evaluating/assessing the criterion for sensitive data in the online environment.

If, however, we accept that sensitivity is determined according to its context and not simply based on an enumerative list under Art. 8(1), then the objectives to critically assess the criterion under Art. 8(1) in this paper will have been achieved. Indeed, Simitis (1999) held that

…sensitivity is no more than a mere alarm device. It signals that the rules normally applicable to the processing of personal data may not secure adequate protection. Its primary consequence is therefore to incite a reflection process the purpose of which is to locate the shortcomings of the existing regulations and to establish the improvements needed. Both the starting point and the range of all considerations are determined by the potential contexts of the processing. They permit the specific risks to be discerned and the antidotes to be designed. Prohibition is hence a possible but by no means a compelling consequence. And even where it appears justified to forbid the use of certain data, the prohibition remains a reaction confined to the context that legitimates and at the same time limits the exclusion of the processing (emphasis added).

Finally, I want to look at the arguments put forward by Simitis (1999) regarding the reduction of exceptions to sensitive data. Although the report was examining the subject in the context of the CoE 1981 it is, nevertheless, relevant for the purposes of the DPD. Simitis argues for a reduction of the present lists of exceptions under the CoE to sensitive data. For example, he considers the issue of consent to exempt the processing of sensitive data.

Already the seemingly incontestable exception heading every list, the consent of the data subject, is anything but convincing. Consent is, contrary to still widespread views, not a master-key opening all doors to any data potential controllers are interested. Employment relationships are only one of many examples demonstrating that consent does not necessarily guarantee a participation of the data subjects enabling them to freely decide whether their data should be processed for purposes known and approved by them….Employment relationships underscore therefore the fallacies of the assumption that consent incorporates and secures the data subjects' power to determine the use of their data.

Moreover, if one considers the current DPD, the main criticism is that the exemptions under Art. 8(2) to the processing of sensitive data are so wide that it brings into question the effectiveness of Art. 8. As illustrated by Simitis (albeit in the context of the CoE Convention on Personal Data 1981),

Terms like public interest or public security are de facto a carte blanche allowing all restrictions finally to be bypassed. The references to both are therefore usually followed by a statement specifying that the conditions of the access have to be regulated by law.

Art. 8(4) DPD provides that

> Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

Under Art. 8(4) DPD member states can extend the exemptions to sensitive data "for reasons of substantial public interest" subject to suitable safeguards. Whether member states have availed themselves of this provision is another matter. The point is that even though sensitive data is processed, it could be exempted under a broad range of headings (as provided under Art. 8(2)).

Simitis (1999) pertinently states that

Sensitivity is reduced to a merely ornamental function where the access can be broadened without any difficulties. Exceptions can certainly not be avoided. But as justified as they may appear, they are intolerable as long as their wording is not precise, their purposes and consequences not clearly determined, the data asked for not confined to really necessary information and the use limited to unmistakably defined controllers.

Space does not permit me to examine all the arguments raised in Simitis's report (1999), but the purpose of considering the issues above is to underscore the dissatisfaction that I have with the current approaches to the regulation of sensitive data under the DPD. In the following section, I want to make some recommendations about this

5. Recommendations

In the light of the arguments about the current approach to sensitive data and in particular, its application on the internet, the question is whether anything can be achieved to address the above issues? Uncertainties still remain on the issue of "profiling" and "identification numbers linking to databases" and whether these activities would fall within Art. 8 of the DPD. Certainly, it can contended that if the act of profiling leads to personal data revealing racial origin, political opinions or religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life then Art. 8 applies. However, what is required is more discussion by data protection authorities and interested parties about "sensitive data" under Art. 8(1) DPD and whether the list could (if at all possible) be amended to take account of technological developments.

Secondly, data protection authorities, legislators and other interested parties should reconsider the approaches towards sensitive data (whether contextualised or purpose-based) particularly in the light of Lindqvist.

Thirdly, there is the subject of enforcement particularly against countries outside the EEA. How do we deal with the case where a data subject within the European Community finds his/her sensitive data being used without his/her knowledge outside the EEA? In other words, are the current mechanisms of co-operation between supervisory authorities adequate or can it be improved? Moreover, there are some countries that do not have data protection laws, but handle personal data (whether sensitive or not) belonging to data subjects within the European Community. Art. 25 of the DPD (on transborder data flows) prohibits the transfer of personal data to countries outside the EEA (termed "third countries") unless the country in question satisfies the adequacy requirement laid down under Art. 25(2) DPD. It does not deal with the collection of personal data by individuals or legal entities outside the EEA that was not directly obtained from the data subjects? For example, X (from a "third country") surfs the internet and finds information about Y, which he subsequently posts an article on the internet including the fact that Y belonged to a religious group. Clearly this is processing of sensitive data. Leaving aside defamation laws, if X's country does not have data protection or privacy laws, then prima facie, it would be difficult to see how Y could seek to enforce his rights. What is recommended is further discussion/co-operation between the EU (acting on behalf of member states) and countries outside the EEA in dealing with the issue of personal information on the internet.

To summarise,

1) Further clarification is needed either from data protection authorities or Art. 29 Working Party about profiling and national identification numbers.
2) Review of the stances towards sensitive data under Art. 8 and its application on the internet by considering the purpose-based/contextualised approach.

3) Further discussion/co-operation between the EU and third countries to personal information on the internet.

6. CONCLUSION

Throughout this paper, I have examined the category for sensitive data under Art. 8(1) taking into account the different approaches to the interpretation of sensitive data. The case of *Lindqvist*,[7] however, raises particular difficulties about the overall application of Art. 8(1) DPD to the internet and questions whether it is time to reform this provision. If we are to instil public confidence in the data protection framework through the DPD, then we (whether as data protection authorities, legislators etc) should ensure that only perpetrators are held accountable. We should refrain from adopting a blanket approach to the application of Art. 8(1) whereby anyone (subject to exemptions) who publishes personal data on the internet could be prosecuted. It is time to sit up and take notice. As the saying goes, "When you make a mistake, don't look back at it long. Take the reason of the thing into your mind and then look forward. Mistakes are lessons of wisdom. The past cannot be changed. The future is yet in your power." (White).

Select Bibliography

1. Bygrave, L.A. (2003) *Data protection law: approaching its rationale, logic and limits*, The Hague: Kluwer Law International.
2. Council of Europe (2005). *Informational self-determination in the internet era*, Retrieved February 2006 (http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Events/T-PD%20_2005_%20RAP%2021%20E.pdf).
3. European Commission. *Commission decisions on the adequacy of the protection of personal data in third countries*, Retrieved February 2006 (http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm).
4. PRIVIREAL. Data protection: countries, Retrieved February 2006 (http://www.privireal.org/content/dp/countries.php).
5. Privacy Exchange. *Japan Privacy Resource*, Retrieved February 2006 (http://www.privacyexchange.org/japan/japanindex.html).
6. Privacy International. *PHR2004 - People's Republic of China*, Retrieved February 2006, (http://www.privacyinternational.org/article.shtml?cmd [347] =x-347-83511).
7. Simitis, S. (1999) *Revisiting sensitive data*, Retrieved February 2006 (http://www.coe.int/T/E/Legal%5Faffairs/Legal%5Fco%2Doperation/Data%5Fprotection/Documents/Reports/W-Report%20Simitis.asp#TopOfPage).

Legislation

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.1995, 31.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, 1981, (European Treaty Series, No. 108)

[7] See n. 1.