BILETA

17th BILETA Annual Conference

April 5th - 6th, 2002.
Free University, Amsterdam.

Data Protection and group companies

M.B.J. Thijssen
Department of Law and Information Technology
University of Nijmegen, the Netherlands

1. Introduction

As a result of the 1995 European Data Protection Directive[1] (the Directive), the United Kingdom and the Netherlands adopted a new data protection act in order to comply with the Directive. The British Data Protection Act 1998[2] (DPA 1998) came into force in March 2000 and the Dutch `Wet Bescherming Persoonsgegevens'[3] (WBP 2001) in September 2001.

On the one hand these acts confer rights to individuals whose personal data are processed. On the other hand they impose obligations on controllers.[4] The Directive defines controllers as persons, companies, public authorities or other bodies who determine the purposes for which and the manner in which personal data are processed.[5]

Under the previous Dutch data protection act of 1989[6] this concept raised the question who could be the controller within a group of companies. Would this be the holding company or each subsidiary?

During the drafting of the WBP 2001 the Minister of Jusitice[7] paid attention to this question. According to the Minister the holding company as well as each subsidiary can be the controller. In case the holding company chooses to be the controller this has to be put down in a contract between the holding company and the affiliated company or in the articles of the affiliated company. However, it must be noticed that the Minister did not state this in the WBP 2001 but only in the Explanatory Memorandum of the WBP 2001.[8]

The option to qualify the holding company as the controller for the other companies within a group does not originate from the European Directive. Therefore the Dutch approach might differ from that in other Member States. At least it differs from the approach in the United Kingdom.

In this paper I will research to what extend the interpretation of the British DPA 1998 differs from the WBP 2001 as far as the processing of personal data in group companies is concerned. The purpose of this paper is to show some consequences that may be caused by an implementation that does not harmonise with the Directive.

2. History

The history of the European Data Protection Directive goes back to 1968. That year the Council of Europe requested the Committee of Ministers to examine whether the European Human Rights

Convention and the national legislations of the Member States offered adequate protection to the right of personal privacy in the light of modern science and technology. The Committee of Ministers concluded that this was not the case.[9]

Thus the Committee adopted two resolutions on data protection.[10] These contained a number of rules that should be observed when personal data were stored in electronic data banks. It was left to the discretion of the Member States in what way they would give effect to these rules. Almost all States decided to do so by legislation.[11]

Afterwards the question raised wether the national legislations offered adequate protection to individuals in case of transborder flows of their personal data. Computers opened new possibilities for the processing of personal data on an international scale. On the one hand individuals should be protected when their personal data flow across borders. On the other hand interference with the free flow of information should be avoided. Therefore the Council of Europe emphasized that the next step should be the reinforcement of national rules on data protection by means of a binding agreement.[12]

In 1981 the `Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'[13] (the Convention)[14] has been opened for signature. The Convention is not intended to be of a self-executing character. Individual rights can not be derived from it. The Convention imposes the duty on states that sign the Convention to implement privacy legislation in accordance with the principles of the Convention.[15]

The British DPA 1984 and the Dutch WPR 1989 have been derived from the Convention. In the United Kingdom the Convention entered into force in 1987. In the Netherlands drafting of the WPR 1989 took more time. Therefore, in the Netherlands the Convention came into force in 1993.

In other Member States it took also quite some time to sign and ratify the Convention. Moreover, article 12 allows states that signed the Convention free to obstruct the transborder flow of personal data adopting higher levels of protection under the guise of protecting individuals.[16] These different levels of data protection may prevent the transmission of personal data from the one Member State to another.

For that reason the necessity for a European Directive, as insisted on by the European Parliament, was recognized by the European Commission in 1990. Five years later the Parliament and the Council adopted the European Data Protection Directive. At the moment Member States are no longer able to prevent the free movement of personal data on grounds related to the protection of the rights of individuals. The approximation of national laws has to result in an equivalent level of protection of the rights of individuals.[17]

3. Definitions

In this section I will explain briefly the most important definitions of both acts. Because the subject restricts itself to the private sector this paper will too.

3.1 Data and personal data

The crucial concept of both DPA 1998 and WBP 2001 is `personal data'. These acts only apply if data can be characterized as personal data.

According to the DPA 1998 `data'[18] means automatically processed information. Manually processed information is considered as data when it is recorded as part of a filing system.[19]

The concept of `data' is not described in the Dutch act. Nevertheless the WBP 2001 does not apply to

an unstructured set containing non-automatically processed personal data.[20]

Data are qualified as `personal data'[21] if the person who controls the data is capable to identify the individual to which those data relate.[22]

Data relate to an individual if the person who controls the data can make a connection between the data and the individual. The individual has to be a living and natural, thus not legal, person.[23] Both DPA 1998 and WBP 2001 call this individual the `data subject'.[24]

A data subject is identifiable if his identity can be established without disproportionate effort. This includes two properties: the nature of the data and the possibility of the controller to establish the identification.[25] In the majority of cases an individual will be identified by knowing the name and the address of that individual.[26]

3.2 Processing

According to both DPA 1998[27] and WBP 2001[28] `processing' means carrying out any operation or set of operations on personal data. Both definitions contain some examples of processing. Using the words of the Information Commissioner[29]: `*The definition in the Act is a compendious one and it is difficult to envisage any action involving data which does not amount to processing within this definition*'.[30] This also holds for the WBP 2001.

3.3 Data controller

`*It shall be the duty of a data controller to comply with the Data Protection Principles*'.[31]

According to the DPA 1998 a `data controller' is a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.[32]

The definition in the WBP 2001 also states who can be the responsible party, i.e. a natural person, a legal person, an administrative body or any other entity. Mostly the data controller will be a company. The employee who busies himself with the processing of personal data is not a controller. [33]

The determination of the purposes for which and the manner in which personal data are to be processed, does not need to be exclusive to one controller. In the United Kingdom as well as in the Netherlands it is possible to share such determination with others. It may be shared jointly or in common.

Determination `in common' is where controllers share a pool of personal data, each processing independently of the other.[34] `Jointly' refers to the situation where determination is exercised by acting together equally.[35] The degree of control exercised by each controller may vary.

3.4 Data processor

According to the DPA 1998 `data processor' means any person who processes personal data on behalf of the data controller. However, a data processor is not an employee of the data controller.[36] The WBP 2001 also states that a data processor is unable to act under the direct authority of the data controller.[37]

The DPA 1998 as well as the WBP 2001 introduce specific obligations upon controllers when the processing of personal data is carried out on their behalf by data processors. According to both laws the controller retains full responsibility for the actions of the processor.[38]

3.5 Third party

Both in United Kingdom and in the Netherlands `third party' means any person other than the controller, the data processor, the data subject or other person authorised to process data on behalf of the controller or the processor, such as an employee.[39]

4. Group companies and the WBP 2001

Under the WPR 1989 it had been questioned whether it was possible to consider the holding company as the controller for the other companies within a group.

The interest to have this question answered lay in the event that when each company had its own responsibility, data flow between these companies had to be construed as third party disclosure. The conditions on third party disclosure were stricter than those which applied on disclosure inside the organisation.[40]

With the drafting of the WBP 2001 the Minster wanted to end this discussion.[41] He accepted that the holding company can become the controller for the other companies within the group if the holding company controls the processing of the data. The other companies within the group are able to use these data without becoming controllers themselves.

This construction is allowed on the condition that it is recorded in a contract between the holding company and the affiliated company or in the articles of the affiliated company.[42]

It has to be noticed that the legislator did not regulate this construction in the WBP 2001 but only in the Explanatory Memorandum to this act.

The situation in which a group of companies runs its business through several separate legal persons, must be distinguished from the situation in which one company runs its business at several locations. In the latter case there is only one controller.

The WBP 2001 no longer distinguishes between disclosure inside and outside the company of the controller. Still, there remains an interest in the possibility to see the holding company as the controller for the other companies within the group.

The possibility plays a part in determining who is responsible in case personal data are processed contrary to the law. The legislator believes it will be more transparent for the data subject if each legal entity is responsible for the processing of personal data within that entity. Because of the transparency it has to be recorded in a contract or in the articles if the holding company becomes the controller for the other companies within the group.

In my opinion it does not diminish the transparency for the data subject when the holding company becomes the controller for the group companies. A data subject will not be informed on the legal structure of the company that processes his data. When personal data are processed within a group of companies the data subject addresses himself to that group and not to a specific legal entity.

The same argument applies when the data subject wants to practice his rights under the WBP 2001.[43] The data subject does not has to know the legal structure of the company in case he wants to practice his rights if the holding company is the controller for the other companies within the group.

The construction also brings about an advantage for the controller. Within a group of companies only the holding company then has to notify to the Data Protection Commissioner[44] instead of each group company.[45]

A serious disadvantage of the possibility to see the holding company as the controller for the group of companies is that it can not be found explicitly in the European Directive. As a consequence it is not to be expected that the idea can be found in the laws of other Member States.

However, it might not be contrary to the purposes of the European Directive to see the holding company as the controller for the processing of personal data within a group of companies. The European Parliament and the Council consider: `*when a single controller is established on the territory of several Member States, particularly by means of subsidiaries*'.[46] This leaves the option that the holding company can be the controller. The subsidiaries will not be seen as establishments if the holding company could not be the controller of these establishments. However, such a reading can not be founded on the Directive itself.

Although the Dutch approach might not be contrary to the Directive, it differs from the approach in other Member States. In section 2 I described the efforts the institutes of the European Union made to achieve a just balance between the protection of personal data and the free flow of information. The institutes of the European Union did intend anything but different national legislation or explanation on the protection of personal data.

Nevertheless, the advantages of the possibility to see the holding company as the controller should not be overestimated. Usually a group of companies will be structured such that the holding company can be liable only if the subsidiaries can not be held liable. The holding company of a group of companies with such a legal structure will probably not be interested to become the controller for the other companies within the group.

5. Group companies and the DPA 1998

In the United Kingdom a holding company seems to be unable to become the controller for the group companies. This can be derived from the fact that `*individual companies who are controllers must notify separately*'.[47]

It is not clear why it is not possible in the United Kingdom for a holding company to become the controller. As we saw in section 3, there are no differences between the DPA 1998 and the WBP 2001 regarding the explanation of the concept of `controller'. So the question is whether a group company that uses the data which the holding company controls, becomes the controller even if that group company does not determine the purposes for which the data are processed. According to the definition of `controller' the group company will not become the controller in that case.

The DPA 1984 also rejected the possibility to qualify the holding company as the controller[48] for the group companies. The supervisory authority stated that: `*If the processing for the group is done by the holding company (...) that company will need to register as a computer bureau*'.[49]

Computer bureaux were `*people or organisations who process personal data for data users or who cause - even indirectly - personal data to be processed for data users, or who allow data users to process personal data on their computer*'.[50]

Qualifying the holding company as a computer bureau did not provide a solution. From the definition flowed that the deploy of a computer bureau did not replace the responsibility from the data user to the computer bureau. A computer bureau wad only limited responsibility for the processing of data. The group companies remained responsible anyway.

The DPA 1998 replaces the concept of the computer bureaux by the concept of `data processor'.[51]

6. Some consequences

It is not possible to discuss all the consequences of an approach that differs from the interpretation in other Member States. So I chose to discuss the consequences that the different approaches bring about as far as article 4 of the Directive is concerned.

6.1 The European Directive

Article 4 of the Directive provides that each Member State has to apply national legislation to the processing of personal data carried out in the context of the activities of an establishment of a controller in that Member State.

If the same controller is established on the territory of several Member States, he must take measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

In case the controller is not established on the territory of any Member State, but he does make use of equipment situated on the territory of a Member State national legislation has to be applied too. [52]

National law does not apply to a controller who is established outside the EEA and only uses the equipment for the transit of the data through a Member State.[53]

On the one hand the Directive provides that national legislation is applicable to the controller who has an establishment on the territory of a Member State. However, on the other hand the Directive provides that the application of national legislation depends on whether the controller is established on the territory of a Member State.[54]

6.2 The WBP 2001

Article 4 (1) WBP 2001 provides that the WBP 2001 applies to the processing of personal data carried out in the context of the activities of an establishment of a controller in the Netherlands.

Suppose a holding company and its subsidiaries are formed under Dutch law. The holding company and the subsidiaries are established in the Netherlands. Only one subsidiary is established in Belgium.

The group companies opt for the Dutch construction. Thus, the holding company becomes the controller of the other companies within the group. Those other companies use the data without becoming controllers themselves.

According to the Directive (the WBP 2001 did not record this rule) the holding company has to take measures to ensure that the subsidiary that is established in Belgium complies with the obligations laid down in Belgian law. It is not stated with which rules of Belgian law the Belgian subsidiary has to comply. We have to assume the subsidiary has to comply with all Belgian rules.

To clarify the problem I draw a distinction between two types of rules. Rules concerning the relation with the supervisory authority and rules regarding the relation between the controller and the data subject.

6.2.1 Relation with the supervisory authority

One of the rules regarding the relation between the supervisor and the controller is the obligation to notify.

In case the Dutch controller notifies, he has to mention the processing done by the Belgian

subsidiary. The controller also has to take measures to ensure that the Belgian subsidiary complies with the obligations laid down by the Belgian law. The Belgian subsidiary also has to give a notification to the Belgian supervisory authority. But according to Belgian law it is not possible for a holding company to notify on behalf of the subsidiary. They are not familiar with the Dutch construction. Thus, it is not possible for the Dutch controller to comply with the Belgian notification rules. The question is whether it is necessary for the Belgian subsidiary to give notification to the Belgian supervisory authority. Probably the answer depends on whether the Belgian subsidiary keeps up a relation with the data subject.

6.2.2 Relation with the data subject

- Rights of the data subject

The relation with the data subject is regulated too. The Directive grants rights to data subjects, such as the right of access to personal data.[55]

Belgian law applies on the subsidiary established on Belgian territory. This implies the data subject has to practice his rights according to Belgian law. The question is whether this is justifiable.

As far as these rights are concerned, it is important whether the Belgian subsidiary keeps up a commercial relation with the data subject. Furthermore, it matters if the data subject knows that he has to do with a Belgian company. If so, it makes no difference to apply Belgian law.

However, suppose the Belgian subsidiary only processes the data. A Dutch subsidiary keeps up the commercial relation with the data subject. Then it might be justifiable to apply Dutch law in stead of Belgian law.

- Liability

Belgian law applies to a subsidiary established on Belgian territory. However, from the Dutch point of view the Dutch holding company can be held liable for the Belgian subsidiary. The Belgian subsidiary can not be held liable, since it is not considered to be the controller.

From the Belgian point of view Belgian law applies. In Belgium it is not possible for a holding company to become the controller for the other companies within the group. Therefore, according to Belgian law, the Belgian subsidiary itself will be liable.

Thus, it is not clear whether Belgian or Dutch law applies in case a data subject holds the Belgian subsidiary liable.

6.3 Company and private law

The WBP 2001 applies as long as the companies are established in the Netherlands, even if the group companies are formed under the law of another state. The Dutch construction can be applied if at least the controller, i.e. the holding company, is established in the Netherlands. Problems may rise because the Dutch construction has to be laid down in a contract between the holding company and the affiliated company or in the articles of the affiliated company. When a company that is not formed under Dutch company law, wants to lay down this construction it is possible that such a contract is or such articles are contrary to national private or company law.

6.4 The DPA 1998

Section 5 (1) DPA 1998 states that the DPA 1998 only applies to controllers who are established in the United Kingdom and who process data in the context of that establishment.[56]

Does this mean that the DPA 1998 only applies to controllers who are resident in the United Kingdom? In other words, does this mean that the DPA 1998 does not apply to establishments on British territory if these are establishments of a controller who is not established on British territory? If so, section 5 (1) DPA 1998 differs from article 4 of the Directive.

Suppose section 5 (1) DPA 1998 differs from article 4 of the Directive and (thus) from article 4 WBP 2001. A holding company and its subsidiaries are formed under Dutch law.[57] The holding company and the subsidiaries are established in the Netherlands. One subsidiary is located on British territory.

The group companies opt for the Dutch construction. The holding company becomes the controller for the other companies within the group. The subsidiaries use the data that the holding company controls without becoming controllers themselves. The holding company has to take measures to ensure that the British subsidiary complies with the obligations laid down by the British law.

Suppose the DPA 1998 only applies to controllers who are established on British territory. The DPA 1998 does not apply to the subsidiary on British territory, because the controller is established in the Netherlands.

In this case there are no difficulties as far as the relation between the controller and the supervisory authority is concerned. The holding company notifies to the Dutch supervisory authority. In case the British subsidiary is liable the Dutch holding company can be held responsible.

Questions will raise about which law applies to the relation between the controller and the data subject. If the subsidiary that is located on British territory keeps up the commercial relation with the data subject it might be justifiable to apply British law. However, according to section 5 (1) DPA 1998 British law does not apply.

Pursuant to the British law each separate legal entity on British territory is the controller of that entity. Therefore, the case I outlined above will not come up in the United Kingdom. However, according to British law it is possible for one company to run its business at several locations.[58] In that case the situation I outlined above might come up.

It must be noticed again that it is not clear if section 5 (1) DPA 1998 has to be explained as I did above. It seems to be just as presumably to explain section 5 (1) DPA 1998 the same as article 4 of the Directive. If so, the same consequences will occur as I mentioned in the example with the Belgian subsidiary.

7. Conclusions

In the Netherlands a holding company is able to become the controller for the other companies within a group. This approach does not originate from the Directive. Neither can it be said that this approach is contrary to the Directive. At least the approach differs from that in other Member States, such as the United Kingdom.

In this paper I described the advantages as well as the disadvantages of the possibility to see the holding company as the controller for the other companies within the group. On the one hand I believe it brings about more transparency for the data subject. On the other hand it brings on a serious disadvantage. After all the Dutch explanation of the Directive differs from the explanation in other Member States.

In this paper I discussed some consequences of the different approach as far as article 4 of the Directive is concerned. The different approach will bring about consequences with regard to other provisions too.[59] The question is whether the advantages of the Dutch approach counterbalance the

efforts the institutes of the European Union made to achieve a just balance between the protection of personal data and the free flow of information.

Bibliography

Berkvens 1989 J.M.A. Berkvens, R.J.M. van der Horst, B.M.F. Verkade (eds.), *Wet persoonsregistraties leidraad voor de praktijk*, Deventer: Kluwer 1989.

Berkvens 2001 J.M.A. Berkvens, *De nieuwe privacywet II, Grensoverschrijdend persoonsgegevens-verkeer,* Euroforum Uitgeverij 2001.

Boswinkel 1991 B.J. Boswinkel, `De registratie-eenheid; de eerstvolgende aanvulling op de WPR?', *Computerrecht* 1991/4, p. 176-183.

Data Protection Registrar 1997 Data Protection Registrar, *The Guidelines*, Fourth series, September 1997, <http://www.dataprotection.gov.uk/dpr/dpdocs.nsf> (January 2002).

Directive 95/46/EC Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*Official Journal* L 281/31).

DPA 1998 Data Protection Act, July 1998, <http://www.hmso.gov.uk/acts/acts1998/80029--a.htm> (February 2002).

Explanatory Report 1981 Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, Strasbourg 1981, European Treaty Series no. 108, margin 4, available at: <http://www.coe.int> see: `Data Protection' (January 2002).

Explanatory Memorandum WBP *Kamerstukken II*, 1997/98, 25 892, nr. 3.

Information Commissioner 2001 Information Commissioner, *Notification handbook, a complete guide to notification*, April 2001, <http://www.dpr. gov.uk/downloads/handbook.pdf> (January 2002).

Information Commissioner 1998 Information Commissioner, *Legal Guidance Data Portection Act 1998*, version 1, <www.dataprotection.gov.uk/dpa98.pdf> (November 2001).

Nugter 1990 A.C.M. Nugter, *Transborder Flow of Personal Data within the EC, a comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the Unites Kingdom and The Netherlands and their impact on the private sector* (diss. Utrecht), Utrecht 1990.

WBP 2001 Wet Bescherming Persoonsgegevens, September 2001, <www.registratiekamer.nl> (February 2002).

WPR 1989 Wet Persoonsregistraties, July 1989.

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L 281/ 31.

[2] Data Protection Act 1998, <http://www.hmso.gov.uk/acts/acts1998/80029--a.htm>

[3] An unofficial English version is available at: <www.registratiekamer.nl>.

[4] Recital 25 Directive 95/46/EC.

[5] Article 2 (d) Directive 95/46/EC, see also section 1 (1) DPA 1998 and article 1 (d) WBP 2001.

[6] The `Wet Persoonsregistraties' 1989.

[7] The Dutch Minister of Justice is comparable with the Lord Chancellor.

[8] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 56.

[9] Explanatory Report, margin 4.

[10] Resolution (73) 22 established data protection principles for the private sector and Resolution (74) 29 established such principles for the public sector.

[11] Explanatory Report, margin 5.

[12] Explanatory Report, margin 8 and Nugter 1990, p. 25.

[13] Strasbourg 1981, European Treaty Series no. 108, available at: <http://www.coe.int>

[14] The Convention has been drawn up within the Council of Europe by experts under the authority of the Committee.

[15] Explanatory Report, margin 38.

[16] Berkvens 2001, p. 352-353.

[17] Recital 9, Directive 95/46/EC.

[18] Section 1 (1) DPA 1998.

[19] Section 1 (1) DPA 1998.

[20] Article 2 (1) and article 1 c WBP 2001.

[21] Section 1 DPA 1998 and article 1 a WBP 2001.

[22] Information Commissioner 2001, p. 11 and *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 47-49.

[23] Recital 24, Directive 95/46/EC, Information Commissioner 2001, p. 11 and *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 46.

[24] Section 1 (1) DPA 1998 and article 1 f WBP 2001.

[25] Recital 26, Directive 95/46/EC and *Kamerstukken II*, 1997/98 25 892, nr. 3, p. 47.

[26] Information Commissioner 2001, p. 12.

[27] Section 1 (1) DPA 1998.

[28] Article 1 b WBP 2001.

[29] The supervisory authority.

[30] Information Commissioner 2001, p. 15.

[31] Section 4 (4) DPA 1998, see for Data Protection Principles: part I of schedule I DPA 1998.

[32] Section 1 (1) DPA 1998.

[33] See definition of `data processor': section 1 (1) DPA 1998.

[34] Information Commissioner 2002, p. 16 and *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 58.

[35] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 58.

[36] Section 1 (1) DPA 1998.

[37] Article 1 e WBP 2001.

[38] Information Commissioner 2001, p. 17 and *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 61.

[39] Section 70 (1) DPA 1998 and article 1 g WBP 2001.

[40] See for the rules applying on third party disclosure: article 11 WPR 1989 and for the rules applying on the disclosure inside the organisation: article 6 (2) WPR 1989.

[41] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 55-56.

[42] *Kamerstukken II*, 1997/98, 25 892, A, p. 5.

[43] Article 35-42 WBP 2001.

[44] Supervisory authority.

[45] Article 27 WBP 2001.

[46] Recital 19 Directive 95/46/EC.

[47] See: Information Commissioner 2001, p. 9.

[48] Section 1 (5) DPA 1984, called `data user'.

[49] Data Protection Registrar 1997, p. 47.

[50] Section 1 (6) DPA 1998 and Data Protection Registrar 1997, p. 5.

[51] Section 1 (1) DPA 1998.

[52] Article 4 (1) c Directive 95/46/EC.

[53] Section 5 (1) b DPA 1998 and article 4 (2) WBP 2001.

[54] See also recital 18 and 19 Directive 95/46/EC.

[55] Article 12 Directive 95/46/EC.

[56] Section 5 (3) DPA 1998 provides who are treated as established in the United Kingdom.

[57] In case the companies are formed under the law of another state the case will not be different. The application of the national laws of the Member States depends on which territory the company is established.

[58] Data Protection Registrar 1997, p. 47.

[59] Such as article 13 of the Directive.