WP 20

Working Party on the protection of individuals with regard to the processing of personal data

Opinion No 3/99 on

Public sector information and the protection of personal data

Contribution to the consultation initiated by the European Commission in its Green Paper entitled "Public sector information: a key resource for Europe" COM (1998) 585

Adopted on 3 May 1999

Opinion No 3/99 on

PUBLIC SECTOR INFORMATION AND THE PROTECTION OF PERSONAL DATA

INTRODUCTION AND PRELIMINARY OBSERVATIONS:

1. The European Commission has submitted a Green Paper entitled "Public sector information: a key resource for Europe" for public consultation[1]. The main objective of the Green Paper is to encourage discussion on how public sector information can be made more accessible to citizens and business, and on whether or not national rules in this area need to be harmonised. The Green Paper appears to have been produced largely as a response to the demands of private players, who want low-cost access to public sector information and who dispute the continuing public sector monopoly in this area.

One of the key aspects of the Green Paper is therefore the availability of public sector information. At issue is a specific category of information held by public sector bodies known as "public" information, which would be made public subject to certain rules or for a particular purpose[2] and based, implicitly or explicitly, on the State's desire for transparency with regard to its citizens[3].

The Green Paper does not ignore the protection of personal data, even though such protection would not appear to be its primary focus.

Paragraph 111 (Chapter III.7, page 16) explicitly states that Directive 95/46/EC on the protection of personal data[4] "establishes binding rules for both the public and the private sectors and [...] must be fully observed in cases of personal data held by the public sector".

Paragraph 114 states that "[t]he emergence of the information society could pose new risks for the privacy of the individual if public registers become accessible in electronic format (in particular on-line and on the Internet) and in large quantities".

However, the Green Paper as a whole contains several ambiguities which cast doubt on the strength of this conviction.

---

[1] Com (1998)585, available at: http://www.echo.lu/legal/en/access.html.

[2] It seems that a distinction can be made between information which must be made public by law, information which is accessible by law, and situations where the issue of publication of, or access to, public sector information is not regulated by law but is raised following a request from individuals or businesses.

[3] This Opinion does not, therefore, deal with the other, broader, meaning of "public", which covers all data processed by public bodies.

[4] 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 protection of personal data and on the free movement of such data, OJ L 281, 23 November 1995, p. 31. Available at: http://www.europa.eu.int/comm/dg15/fr/media/dataprot/index.htm.

First, the use of the term "publicly available" creates the impression that information, by virtue of its availability, can be used for any purpose. The principle of purpose, which is a cornerstone of our data protection legislation, sits uneasily with the adjective "available". Furthermore, the principle of honesty in data collection is ensured in particular by the requirement of security of processing, but could suffer if data are made public without prior discussion or precautions being taken. It is therefore advisable that the phrase "publicly available" be replaced by a more suitable and unambiguous wording (such as "publicly accessible").

Secondly, Question 7 ("Do privacy considerations deserve specific attention in relation to the exploitation of public sector information?", page 16) might lead one to think that Directive 95/46/EC is not as definite as one might have imagined on this point, while at the same time paragraph 111 states that Directive 95/46/EC "achieves the necessary balance between the principle of access to public sector information and the protection of personal data". These ambiguities need to be removed.

2. The objective of this Opinion is to provide input for the discussion on the protection of personal data, a dimension which must be taken into consideration when undertaking to grant greater access to public sector data, where such data relates to individuals. However, the Opinion does not claim to provide answers to all of the questions raised by the need for a balance between improved access to public sector data, based on a desire for increased transparency by the State with regard to its citizens, on the one hand, and the protection of personal data as defined by Directive 95/46/EC, on the other.

So this Opinion does not deal with issues raised in the Green Paper which go beyond the issue of making public sector information available to third parties, such as the viewpoint expressed in paragraph 56 (Chapter II.2, page 9), for example, that "[t]he use of new technologies can considerably increase the efficiency of the collection of information. It gives public bodies the possibility to share available information when this is in conformity with data protection rules".

Drawing on Directive 95/46/EC and on practical illustrations using the best-known public registers of personal data, this Opinion aims to provide a first set of pointers to be considered when taking real-life decisions. These pointers and practical examples from a variety of Member States are intended to show how, in the information society, the rules on data protection should be taken into account with regard to data from public registers. While it cannot claim to ensure protection in every case, this Opinion also aims to point to some of the technical and organisational measures which can help to balance publication of these data against compliance with the provisions on personal data protection and in particular the provisions relating to the fundamental principle in this area, i.e. the purpose for which the data are made public.

I - THE RULES ON DATA PROTECTION APPLY TO PERSONAL DATA WHICH HAVE BEEN MADE PUBLIC

The accessibility of public sector information advocated in the Green Paper, particularly through computerisation, raises the issue of how these data are used. Their usage cannot be prohibited as this would run contrary to trends in society. Nor is prohibition the intention of

our data protection legislation: its task is to regulate the computerisation of society, not to proscribe it.

It is perfectly clear from the wording of our data protection legislation that it applies to personal data made publicly available: even after personal data are made public, they are still personal and must therefore be protected.

This assertion requires an examination of exactly what protection is afforded to personal data made public. In this regard, Directive 95/46/EC can provide some of the answers.

A - 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

The rules of the Directive cover the principle of the right of public access to administrative documents[5] and other factors which are relevant to the discussion[6].

The principle of purpose requires that personal data are collected for specific, explicit and legitimate purposes and are not subsequently processed in a manner which is incompatible with these purposes.[7] This principle therefore plays a key role in the accessibility of personal data held by the public sector.

In particular, a case-by-case examination is required of the extent to which a law makes publication or public access to personal data mandatory or permissible. Is the law intended to ensure access to the data in their entirety with no time limitation? Can the data be used for any purpose, regardless of the initial purpose or, conversely, does the law allow only some parties to access the data and/or does it require that the data be used for a purpose linked to the initial purpose for which they were made public? Consequently, personal data to be made public do not constitute a homogeneous category which can be dealt with uniformly from a data protection point of view. Instead, a step-by-step analysis is needed of the rights of the data subject and the right of the public to access the data respectively. While there may be public access to data, such access may be subject to certain conditions (such as proof of legitimate interest). Alternatively, the purposes for which the data may be used, for example for commercial purposes or by the media, may be restricted. The examples below illustrate these points.

At this point it is worth mentioning that regardless of whether or not personal data are published, data subjects always has the right to access their data and, where necessary, to require that they be rectified or erased if they have not been processed in accordance with the Directive, and in particular if they are incomplete or inaccurate[8].

---

[5] See recital 72. It is important to note for this discussion that the Directive does not define "administrative documents". However, they can be considered in a broad sense to include at least the "administrative information" defined in the Green Paper proposal for a classification of information (paragraph 73 *et seq*, page 11).

[6] See Article 10 and recital 37 of Directive 95/46/EC on achieving a balance between the right to privacy and the rules on freedom of expression. See also Recommendation 1/97 of the Working Party on "Data protection law and the media", adopted on 25 February 1997 (Document No 5012/9, available in the eleven official languages at http://www.europa.eu.int/comm/dg15/fr/media/dataprot/index.html).

[7] For details see Article 6(1b) of Directive 95/46/EC.

[8] See Article 12 of Directive 95/46/EC.

A number of provisions of the Directive refer explicitly to the public nature of data. Two of these provisions are worth examining in some detail.

Article 18(3) concerns the obligation to notify the supervisory authority of the processing of data and states that an exception may be made in the case of a register "which according to laws or regulations is intended to provide information to the public and which is open to consultation ... by the public in general". But it should be noted that recitals 50 and 51 of the Directive specify that exemption or simplification only applies to processing operations whose sole purpose (first condition) is the keeping of a register intended, according to national law, to provide information to the public (second condition) and open to consultation by the public or by any person demonstrating a legitimate interest (third condition). However, such derogations do not release the controller from any of the other obligations resulting from the Directive.

Finally, Article 26(1f) contains a derogation from the requirement of an adequate level of protection, where data are transferred to a third country which does not ensure an adequate level of protection "from a register ... which is open to consultation ... by the public". However, recital 58 of the Directive limits the scope of such transfer by specifying that it should not involve the entirety of the data or entire categories of the data contained in the register and, where appropriate, the transfer should only be made at the request of persons having a legitimate interest.

It is clear from the provisions and recitals referred to above that personal data protection considerations should not be used to prevent citizens from accessing administrative documents under conditions laid down in national legislation. However, the Directive is not intended to remove all protection from publicly-accessible data either.

The discussion on whether the national rules on access to public sector information need to be harmonised should in any case take account of the harmonised rules on the protection of personal data and the associated national transposition measures.

In addition to the Commission's task of monitoring the application of the Directive, the Working Party set up under Article 29 of the Directive shall undertake a concrete examination of the impact of the national measures implementing Directive 95/46/EC in specific cases, which could bring to light divergences at national level.[9]

B - Examples of how a balance is struck between the rules on personal data protection and the right of access to public sector information

Some national legislation only allows public sector information to be used for certain purposes. Access to certain data may be prohibited, certain uses may be prohibited, or conditions may be imposed on access.

[9] See Articles 29 and 30 of Directive 95/46/EC.

The computerisation of data and the possibility of carrying out full-text searches creates an unlimited number of ways of querying and sorting information, with Internet dissemination increasing the risk of collection for improper purposes. Furthermore, computerisation has made it much easier to combine publicly available data from different sources, so that a profile of the situation or behaviour of individuals can be obtained[10]. In addition, particular attention should be paid to the fact that making personal data available to the public serves to fuel the new techniques of data warehousing and data mining. Using these techniques, data can be collected without any advance specification of the purpose, and it is only at the stage of actual usage that the various purposes are defined. So all of the technological possibilities with regard to data usage need to be considered[11].

This is why it is important to check, on a case-by-case basis, what the negative repercussions on individuals might be, before taking any decision on computerised dissemination. In some cases a decision will have to be taken either not to release certain personal data, to let the data subject decide, or to impose other conditions.

1 - Databases of court decisions:

Paragraph 74 of the Green Paper (page 11) refers specifically to court cases to illustrate the notion of "information that is fundamental for the functioning of democracy". This raises a basic question, namely: do we really imagine that putting every judgment from every court on the Internet will not harm individuals?

If special precautions are not taken, case-law databases, which are legal documentation instruments, can become information files on individuals if these databases are consulted to obtain a list of the court judgments on a specific individual rather than to find out about case-law, for example.

In an opinion delivered on 23 December 1997, the Belgian Commission for the Protection of the Right to Privacy (*Commission de la Protection de la Vie Privée*) strongly emphasised this point, stating that advances in technology mean that greater caution must be exercised when naming the parties in case-law chronicles. The Commission proposed that, if complete

[10] Note that the use of such technologies also enables the State to establish such profiles.

[11] A further example of this is that it is possible to obtain negative information about individuals more easily by combining two databases electronically, e.g. the names of people who are not entitled to vote can be obtained by combining the population register (where it exists in computerised form) with the electoral rolls.

anonymity is not an option, court decisions which are accessible to any group of public users should not be indexed by name, thereby preventing searches from being made on the basis of the names of the parties.

The Italian Commission for the Protection of Personal Data[12] is considering putting forward a proposal at national level to the effect that the parties should be entitled to prevent their names from being published in case-law databases. They could exercise this right at any time and have their names removed when computerised databases are updated. Existing paper publications would not be affected by this entitlement.

The French Ministry for Justice wishes to disseminate case law databases on the Internet and has stated in the specifications that the parties to court decisions must remain anonymous.

2 - Certain official texts:

The Internet has caused an information explosion at international level and a corresponding increase in information sources. This globalisation of information may generate a particular type of risk. The distribution of information which is legitimate public information in one country can seriously endanger the privacy or physical safety of individuals if disseminated worldwide. In some countries, for example, publication of the names of naturalised persons is mandatory. This is the case in France where, on the advice of the National Commission for Information Technology and Civil Liberties (*Commission Nationale de l'Informatique et des Libertés* -CNIL), the Government has excluded lists of naturalised persons from the version of the Official Journal published on the Internet, in order to ensure that certain nationals who have given up their original nationality are not subjected to retaliation.

In certain cases, therefore, the desire of the State - and in particular of its nationals - for transparency sits uneasily with the global dissemination of such data.

3 - Other instances of the imposition of conditions on the dissemination of personal data which have been made public, in order to protect data subjects:

The conditions of access to personal data contained in registers vary greatly, depending on the regulations governing them. These conditions include partial access, proof of legitimate interest and the prohibition of commercial usage.

In Germany, for example, all lists of candidates in Federal elections must include the surname, forename, profession or status, date and place of birth, and address of each candidate. But in the lists which the returning officer responsible for organising federal elections at local or *Land* level makes public before the ballot, the date of birth is replaced by the year of birth.

[12] Garante per la protezione dei dati personali

In Italy, the legislation governing the population register held by each municipality prohibits data from being passed to private bodies and requires any public authority requesting data to provide proof of legitimate public interest.

The electoral register in France is public so that the entries can be checked for validity. By law, all candidates and political parties may use the register for political purposes but commercial usage is prohibited. It is inconceivable that the electoral lists would be published on the Internet.

Also in France, personal data in the cadastral register are public, but may not be used for commercial ends.

In Greece, where the cadastral register is organised on the basis of an alphabetical index of property owners, the current system will be replaced by an index based on the properties themselves in order to prevent users from carrying out searches on the property owned by a single individual. Access to the cadastral register requires proof of legitimate interest.

II - THE NEW TECHNOLOGIES CAN HELP STRIKE A BALANCE BETWEEN THE PROTECTION OF PERSONAL DATA AND THE PUBLICATION OF SUCH DATA

In addition to promoting access to public data, in particular by providing on-line access, the new technologies and some of the accompanying administrative measures can also help to ensure compliance with the main principles of data protection, such as end purpose, the principle of information, the right to object and the principle of security. However, these technologies do not provide an absolute guarantee against abuses of the principles of personal data protection described above.

A - The technical conditions for access to public sector information must help ensure compliance with the principle of purpose

Given the conditions of public access to computerised data, it is obviously very difficult to guarantee in practice that data are actually used for the stated purpose, but properly thought-out and targeted use of technology can help attain this objective. This means, however, that in each individual case the query conditions must be defined and checked. The following principle should apply: "anyone may read any individual data set to the extent authorised, but not all data sets in their entirety". The search criteria must be chosen in such a way that it is impossible to misuse the data in normal usage. It is also necessary to check whether it is possible to get around the obstacle using additional information from other sources.

To prevent data from being used for purposes other than that (those) for which they were made public, on-line consultation of databases can be restricted. Such restrictions would be

applied on a case-by-case basis and might involve, for example, limiting the field of the query or the query criteria.

In France, for example, any person who knows the name, date and place of birth of an individual can access their birth certificate. The National Commission for Information Technology and Civil Liberties has made on-line access to birth certificates subject to the condition that the on-line request includes all of this information. Thus, by laying down criteria restricting the scope of database queries, large-scale collection of data from these registers for commercial purposes can be prevented and compliance with the principle of purpose can be ensured.

Again in France, it used to be possible to query the computerised version of the telephone directory using the first few letters of the surname, thereby making it easier to download the entire directory and use it for commercial purposes against the wishes of some subscribers who had objected to such usage. Possible abuses of purpose in this manner were headed off by making this type of query impossible on Minitel and the Internet.

In the Netherlands, the telephone directory on CD-Rom has been designed in such a way that users cannot obtain people's names and addresses simply by knowing their telephone number (it is impossible to query the database using the telephone number alone).

Similarly, it should not be possible to query business registers using the person's name alone, because this would allow users to find out all of the business interests of a single individual.

B. The use of technical tools to prevent the automatic capture of on-line data should be encouraged

An example of such a tool is the Robots Exclusion Protocol, whose goal is to prevent all or some of the pages in a website from being indexed automatically by a search engine. But such a protocol can only be effective if website designers and Internet users know that it exists and if search engines comply with it. Some search engine producers say that they adhere to this protocol.

III. Commercial usage

Personal data held by the public sector are initially collected and processed for specific purposes and, normally speaking, on the basis of certain rules. In some instances the provision of data is mandatory and in other cases information must be supplied in order to gain access to a public service. Therefore, data subjects do not necessarily expect that their personal data will be made public and used for commercial purposes. This is one of the reasons why some national legislation permits access to public sector information, including personal data, but prohibits the use of such data for commercial ends[13].

[13] See Annex 1 of the Green Paper: Current situation in Member States regarding legislation and policy on access to public sector information, page 20 *et seq.*

From the point of view of Directive 95/46/EC[14], the question arises as to whether commercial usage should be viewed as incompatible with the original purpose for which the data were collected and, if so, under what conditions commercial usage might nevertheless be permitted.

If public sector information is to be published and marketed[15], certain rules must be obeyed. In each individual case, a balance needs to be struck between the right to privacy and the commercial interests of private operators.

Directive 95/46/EC recognises the right of data subjects to be informed about the processing of data concerning them and stipulates that at the very least they have the right to object to legitimate processing. Data subjects must therefore be informed about the commercial usage of data concerning them and must be able to object to such usage by simple and effective means[16].

Much remains to be done in this respect. Given the profusion of data dissemination sources, the large number of operators and the possibility of downloading data, the notion of a one-stop-shop for data protection is gaining ground, meaning that data subjects would not have to object to each operator individually. In several European countries, people listed in the telephone directories can avail themselves of this option.

For the same reason, the National Commission for Information Technology and Civil Liberties[17] has recommended that all publishers of directories should identify the subscribers who have exercised their right to object to their details being used for commercial purposes. The publishers should do this on every medium on which their directories are published (hard copy, CD-Rom, Minitel or Internet).

The idea of a one-stop-shop would appear to be essential both to ensure that people's rights are respected and to act as a reference point for commercial operators wishing to use personal data.

To achieve a balance between the right to privacy and the commercial interests of operators, it may also be necessary to obtain the data subject's consent[18] or even to introduce legislation or regulations, as the following example shows.

In an opinion on the use of planning permission data for commercial purposes, Belgium's Commission for the Protection of the Right to Privacy considered that such usage could only be lawful if the new purpose (in this case the use of data processed by public authorities for

[14] See Article 6(1b) of Directive 95/46/EC.

[15] It should be noted that some people consider that since personality profiles can be assembled by combining data from various sources, the use of personal data for commercial purposes should be banned or at least restricted and infringements punished. As regards personal data from official sources, there should be no exception to the obligation to inform the data subject (Article 11 of the Directive).

[16] See Articles 10, 11 and 14 of Directive 95/46/EC.

[17] Commission Nationale des Libertés et de l'Informatique, France.

[18] See Articles 2(h), 7(a) and 8 of Directive 95/46/EC on the definition of consent and the requirement of specific forms of consent in some cases.

commercial purposes) had a legal or statutory basis defining it in exact terms. Without such a basis, the Belgian Commission considered that the interests served by passing on data to third parties did not override the data subject's right to privacy. Another possibility mentioned in the opinion was to obtain the data subject's consent for commercial usage. Data subjects must have given their consent unambiguously and in full knowledge of the facts, taking into account the fact that anyone applying for planning permission is required to submit a file which meets certain stipulations.

Later on in the same opinion, the Belgian Commission refers to the obligation to inform data subjects of processing concerning them, and stresses in particular that they are entitled to object to such processing, on request and without charge, if the data are to be used for direct marketing purposes.

CONCLUSION:

Public access to data does not mean unfettered access: all Member States base their legislation on this philosophy. When personal data are made public, either by virtue of a regulation or because the data subject himself authorises it, the data subject is not deprived of protection, *ipso facto* and forever. He is guaranteed such protection by law in accordance with the fundamental principles of the right to privacy.

In order to strike a balance between the right to privacy and the protection of personal data on the one hand, and the right of the general public to access public sector data on the other, the Green Paper consultation and conclusions must take account of the following factors and issues:

- a case-by-case assessment of whether personal data can be published/should be accessible or not, and if so, under what conditions and on which media (computerised or not, Internet dissemination or not, etc.);
- the principles of purpose and legitimacy;
- the obligation to inform the data subject;
- the data subject's right to object;
- the use of the new technologies to help protect the right to privacy.

These factors should be taken into account not just in situations where publication or access is already regulated, but also in situations where regulation does not appear necessary, with a view to satisfying the general public's demand for access to public sector information, including personal data.[19]

[19] See footnote on page 2.

The Working Party looks forward to the European Commission's conclusions on the current consultation process, and would be extremely interested in contributing to future work in this area, including the issue of third party access to public information, which strictly speaking goes beyond the scope of the Green Paper[20].

Brussels, 3 May 1999

On behalf of the Working Party

Peter Hustinx

Chairman

[20] See, for example, the earlier reference to paragraph 56 (page 9 of the Green Paper) on the possibilities of collecting and sharing information, and paragraph 123 (page 18) containing a proposal for the exchange of information between public bodies.