



**5003/00/EN/Final
WP 44**

Opinion 5/2001

**On the European Ombudsman Special Report to the European Parliament
following the draft recommendation to the European Commission
in complaint 713/98/IJH.**

Adopted on 17 May 2001

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC. The Secretariat is provided by:

The European Commission, Internal Market DG, Functioning and impact of the Internal Market. Coordination. Data Protection.
Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgium - Office: C100-6/136
Internet address: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 ;

Having regard to Articles 29 and 30 paragraphs 1a) and 3 of that Directive ;

Having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof ;

HAS ADOPTED the present Opinionⁱ.

1. INTRODUCTION

The Working Party has been made aware that the European Parliament will be discussing the issue of public access to documents and privacy raised by the Special Report submitted by the European Ombudsman to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH. The European Parliament has also been requested to adopt this recommendation as a resolution.

The Working Party is aware that the further development of this specific file will take place within the inter-institutional framework of the Community. However, according to article 30 of Directive 95/46/EC, the Working Party may, on its own initiative, make recommendations on all matters relating to the protection of personal data in the Community. The Working Party finds that a Resolution of the European Parliament with this regard, as sought by the Ombudsman, may have a considerable impact on the protection of individuals with regard to the processing of personal data at Community level. The Working Party considers its duty to deliver its opinion on the main legal aspects of a question concerning personal data protection. The scope of this document is therefore limited to the question of personal data protection and public access to documents within the Community institutions and bodies.

2. THE QUESTION OF PRIVACY AND OPENNESS IN GENERAL TERMS

The Working Party would like to recall its Opinion No 3/99 on Public sector information and the protection of personal data. Personal data contained in a official document or held by a public administration or body are still personal and must therefore be protected according to the data protection legislation, as far as the processing of such data falls within the scope of this legislation. In particular, in the case of the Commission, the data protection Directive 95/46/EC (*“the Directive”*) applies pursuant to article 286 of the Treaty establishing the European Community. It should be noted that on the basis of this article, the European Parliament and the Council have subsequently adopted Regulation 45/2001/CE of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such dataⁱⁱ.

On the other hand, the right of the citizens to have access to public documents is an important element for accountability of the administration vis-à-vis citizens and for transparency in decision-making process by public bodies. At Community level, the right of access is enshrined in article 255 of the Treaty.

All countries of the European Union and the Community institutions are equally committed to both rights as cornerstones of a democratic society. The Charter of fundamental rights of the European Union recognises the right to the protection of personal data in article 8 thereof, and the right of access to documents in article 42.

Both rights being of the same nature, importance and degree, they should be enacted jointly, and a balance will have to be found for each particular case concerning a request for access to a public document containing personal data. The harmonisation of these two rights for each particular situation will result in the public authority granting such access or rejecting it. Therefore, it should not be assumed that there exists in principle and necessarily a conflict between these two rights. Accordingly, recital No 72 of the Directive allows for the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive.

3. ASPECTS RELEVANT FOR THE PROTECTION OF PRIVACY CONCERNING THE PUBLIC DISCLOSURE OF PERSONAL DATA HELD BY A PUBLIC ADMINISTRATION OR BODY.

From the point of view of the protection of privacy, the disclosure to third parties of personal data collected and held by a public administration or body is to be considered as processing of personal data in the sense of the Directive. According to the definition contained in article 2 b) thereof, *'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, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*

The analysis that follows is relevant when this processing of personal data falls within the scope of the Directive and of national laws on data protection pursuant to it. In particular, article 3 of the Directive states that it shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. Further, article 2 sets out that for the purposes of the Directive, 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. Where the Directive does not apply, the privacy of individuals is protected by article 8 of the European Convention on Human Rights.

Under those circumstances, the processing of personal data is subject in all cases to the requirements set in article 6 of the Directive. In particular, mention should be made to letters a) and b) thereof, where it is prescribed that personal data must be:

(a) processed fairly and lawfully.

Public disclosure of personal data held by a public administration or body should thus be fair and lawful. Attention must therefore be paid in each particular case to see that disclosure is not unfair to the data subject considering the circumstances of each situation. Disclosure should further not be unlawful, for instance because it would breach a legal obligation placed on the public administration or body, such as a duty of confidence arising from the nature of the data and the circumstances surrounding the data collection.

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes [...].

At this point, it is important to determine whether the processing of personal data held by a public administration or body and consisting in disclosing these data to third parties

belonging to the public in general can be considered as not incompatible with the purpose for which those data were originally collected and further processed.

The response will require a detailed analysis of each type of the purpose of the collection and further processing of personal data on a case by case basis. The assessment will normally be made by the controller. It may also be made by regulations for certain categories of data or documents. The assessment will have to take into account the compulsory or voluntary basis of the data collection; the kind of personal data processed; the situation of the data subject and the potential consequences of public disclosure of the data for him or for her. Although the principle of openness in administration is an element to be considered in favour of such compatibility, the need for an analysis of the circumstances for each situation lets us reject the argument that public disclosure of such data is unconditionally and automatically compatible with the purpose for which data were collected and further processed, only because the controller is a public administration or body and on the sole basis of that principle of openness.

4. LEGITIMACY OF PUBLIC DISCLOSURE OF PERSONAL DATA

In general, the processing of personal data consisting in making such data available to the public would need to be legitimate according to one of the reasons set out in article 7. These are the following, according to the order of presentation in the Directive:

(a) the data subject has unambiguously given his consent.

In such cases, the public administration or body may proceed to the public disclosure of personal data. However, where data subjects have not given their consent to such disclosure (and even more, when this consent has been explicitly refused), access by a third party to personal data held by the administration may only take place if any of the other reasons for legitimate processing applies.

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

On this basis, the public administration or body which holds the data may disclose them to a third party who actually acts as an agent of the administration for the implementation of a contractual relationship. This is for instance the case of personal data relating to civil servants being disclosed to a bank through which salaries are paid. However, the case of disclosure to any third party belonging to the public in general would be difficult to justify under this heading.

(c) processing is necessary for compliance with a legal obligation to which the controller is subject.

Public administration or bodies are sometimes obliged by Law to disclose personal data they hold to third parties upon request. This is for instance the case of personal data contained in a public register which is open to any person justifying a legitimate interest, like the Real Estate Register.

The Working Party would like to underline that legislation on public access to administrative documents in most European countries establishes the general obligation for the administration to grant public access to documents, with the exception of, or with due regard being made to, the rules on privacy and data protection. In some countries, the Laws on public access allow to refuse it if, for the particular case concerned, other interests, such as privacy, are found to prevail. Legislation may provide in some cases for disclosure to the public in general, or only to persons demonstrating a legitimate interest in other cases. It may also set out different rules for different kinds of data or for different categories of data subjects concerned. In some countries, for instance, public disclosure

of personal data is granted on a broader basis when the data refer to civil servants and relate to their functions, than when those data refer to common citizens in general.

In the case of the Commission, it is itself subject to rules that impose for it to take into account both the principle of openness and the protection of privacy. In fact, the rules regarding public access to documents in force at the time of the request that gave rise to the complaint to the Ombudsmanⁱⁱⁱ explicitly stated that the Institutions would refuse access to any document where disclosure could undermine the protection of the individual and of privacy. Furthermore, the Treaty establishing the European Community specifically provides in article 255 that limits on grounds of public or private interest governing the right of access to Community documents shall be determined, while prescribing in article 286 that Community acts on the protection of individuals with regard to the processing of personal data shall apply to the Community institutions.

Given that the obligation of administrations to grant public access to documents is limited by their obligation to protect personal data, an unrestricted, automatic, unfettered public disclosure of personal data held by the administration without taking into account the need to protect privacy would no longer be in line with the provisions of Laws governing public access to documents, since it would no longer respect the exception laid down by the same legislation. It would therefore not be compliant with a legal obligation to which the administration would be subject, and thus would not be legitimate on the basis of this heading. In other words, the compliance with a legal obligation cannot be used as a proper ground to make automatic, unrestricted public disclosure of personal data legitimate according to the Directive.

On the contrary, the joint reading of most legislation on public access and on data protection prescribe the need to strike a balance between the two rights. This imposes an analysis of the circumstances on a case by case basis, in order to conclude which of the two rights or interests should prevail each particular situation, and therefore whether the request for access should be satisfied or rejected.

(d) processing is necessary in order to protect the vital interests of the data subject.

On this basis, the public administration or body which holds the data may publicly disclose them when dissemination of such data is needed to protect the vital interest of data subjects. This is for instance the case of public authorities disclosing data relating to missing persons, insofar as widespread knowledge of those data may help find the person or protecting the data subject.

In most cases of requests for access to personal data, though, this ground for justification is not likely to apply.

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

The Working Party points out that, in general terms, it is difficult to distinguish such situations from the ones covered under point c), and therefore the arguments exposed there may apply. In fact, if public disclosure is necessary for the performance of a task carried out in the public interest by a public administration, then the legislation itself will normally have provided for a corresponding obligation to disclose such data, according to the principle of Rule of Law. However, there may be cases where, although public disclosure is not a specific legal obligation for a public body, it cannot reasonably meet the requirements placed on it by law if it does not disclose personal data it holds. Disclosure will then be a necessary consequence of performance of the task, even if it does not constitute a specific obligation in Law.

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

The Working Party notes that this heading contains a general clause that imposes a balance to be found between the right of data subject to privacy, on the one hand, and on the other hand, other legitimate interests, such as the right to public access to administrative documents. The Directive requires that an assessment of the rights and interests present in any given situation be made on a case-by-case basis and taking into account all circumstances surrounding each situation. It would be unacceptable to place *a priori* the right of access to documents above the right of privacy, as it would be equally wrong to do it the other way round. The prevalence of the right of access above the right to privacy, or inversely, of privacy above openness, should be the result *a posteriori* of a thorough analysis of each case. If the right to public access is found to prevail, public disclosure of personal data should be made. If privacy is found to prevail, public disclosure of personal data should be refused.

The aforementioned considerations are pertinent when article 7 of the Directive applies. However, it should be remembered that the Directive includes specific provisions for special categories of data. In particular, article 8 thereof prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning sex and health life, while providing for a limited number of justified exceptions.

5. CONCLUSIONS

The response to the question of whether *a public administration or body is obliged to public disclosure of personal data it holds in cases where the data subjects have explicitly refused their consent to such disclosure* should take into account the following considerations which are relevant from the point of view of the protection of the fundamental right to privacy. These considerations apply when the processing of personal data carried out by the public administration or body is carried out by automatic means, or it is performed otherwise than by automatic means on personal data which form part of a filing system or are intended to form part of a filing system.

- An analysis should be made of whether public disclosure is to be considered a fair and lawful processing, according to the circumstances present in each case. Furthermore, disclosure should not be incompatible with the original purpose for which personal data were collected and further processed by the public administration or body. Such analysis should be made on a case-by-case basis and in particular take into account the compulsory or voluntary basis of the data collection; the kind of personal data processed; the situation of the data subject and the potential consequences of public disclosure of the data for him or her.
- While the processing of sensitive data is subject to the specific provisions of article 8 of the Directive, public disclosure of personal data held by a public administration or body must in general be covered by one of the following reasons set out in article 7 of the Directive in order to make it legitimate:
 - data subject have unambiguously given their consent (*article 7, point a*); obviously, if data subject have not given their consent (and even more, when this consent has been explicitly refused), this justification disappears.
 - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (*article 7, point c*).

However, the case of disclosure of personal data held by the public administration or body to any third party belonging to the public in general would be difficult to justify under this heading.

- processing is necessary for compliance with a legal obligation to which the controller is subject (*article 7, point c*).

It should be noted, though, that the obligation to public disclosure imposed by the legislation on public access to administrative documents does not establish an absolute obligation of openness. It rather makes the obligation to grant access to documents subject to due regard being made of the right to privacy. Therefore, it does not justify unlimited or unfettered disclosure of personal data. On the contrary, a joint reading of legislation on public access and on data protection normally imposes that an analysis of the circumstances surrounding each situation is made on a case by case basis, in order to strike a balance between those two rights. In particular, as a result of such assessment, legislation on public access may provide for different rules to apply to different categories of data or different kinds of data subjects.

- processing is necessary in order to protect the vital interests of the data subject (*article 7, point d*).

In most cases of requests for access to personal data, though, this ground for justification is not likely to apply.

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed (*article 7, point e*).

In general terms, it is difficult to distinguish such situations from the ones covered under article 7, point c). However, there may be cases where, although public disclosure is not a specific legal obligation for a public body, it cannot reasonably meet the requirements placed on it by law if it does not disclose personal data it holds.

- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1) (*article. 7, point f*).

The necessary assessment of the rights and interests present in any given situation should be made on a case-by-case basis and taking into account all circumstances surrounding each situation. If the right to public access is found to prevail, public disclosure of personal data should be made. If the right to privacy is found to prevail, public disclosure of personal data should be refused.

Done at Brussels, 23 May 2001

For the Working Party

The Chairman

Stefano RODOTA

ⁱ The Data Inspection Board, Sweden, opposes the document for the following reasons. Firstly, the Board thinks that general conclusions such as those drawn in the Opinion should be based on a more comprehensive analysis. Furthermore, the conclusions of the document imply, in the Board's view, that the right of public access to official documents is subordinate to the Data Protection Directive. This does not constitute an appropriate balance between the right of public access and the right of data protection.

The Danish and the Finnish members of the Working Party support this view.

ⁱⁱ OJ L 8 of 12.1.2000

ⁱⁱⁱ Commission Decision of 8 February 1994 on public access to Commission documents (94/90/ECSC, EC, Euratom), including the Annex consisting of the Code of conduct concerning public access to Commission and Council documents.