EDPS - European Data Protection Supervisor

Public access to documents and data protection

Background Paper Series

Summary

July 2005

n°1

The European Data Protection Supervisor has issued a paper with guidelines for dealing with requests for access to public documents containing personal data. This brochure only contains a short summary of the paper. The complete text of the paper and a checklist for officials dealing with requests for access are available at the EDPS website: www.edps.eu.int

Introduction

Public access on the one hand and privacy and data protection on the other, are fundamental rights which are laid down in a wide range of legislation at the European level. These rights are deeply rooted in the constitutional traditions of the Member States and enjoy substantial public support. They are also essential elements of "good governance". In 2001, two Regulations have been adopted that oblige EU-institutions and bodies to respect these rights: Regulation (EC) 45/2001 (hereafter: "Data Protection Regulation") and Regulation (EC) 1049/2001 (hereafter: "Public Access Regulation").

There is no hierarchical order - and often no tension - between the two rights. However, as the objective of the Public Access Regulation is to foster access to all documents, whereas the Data Protection Regulation must guarantee the protection of personal data, a tension can arise in some cases. The simultaneous application of the two Regulations has sometimes been perceived as a challenging area. The European Data Protection Supervisor (EDPS) therefore decided to publish a paper which sets out to show that the rights must be seen as complementary - rather than contrary - to each other.

The aim of the paper is to give practical guidance in cases where one needs to establish whether a document which contains personal data should be disclosed to a third person, e.g. in reply to questions on employees or attendance of meetings, or in relation to a complaint procedure, or when considering the publication of a list on the Internet.

The simultaneous application of the two Regulations

The Public Access Regulation responds to the fact that in most democratic societies there is a general interest in the disclosure of documents of public authorities. The Regulation therefore strives at the widest possible degree of public access to documents for any EU citizen, as well as for natural and legal persons residing or having their registered office in a Member State.

The right to public access is limited by a number of exceptions, one of which is essential for the paper, since it relates to privacy and data protection. Article 4 (1) (b) states:

The institutions shall refuse access to a document where disclosure would undermine the protection of […] the privacy and integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data.

The initial words of Article 4 (1) (b) are absolute: disclosure shall be refused. However, the other elements contain conditions that call for a concrete and individual examination of the contents of the document. When doing that, all relevant elements have to be taken into account.

Analysing the Article 4 (1) (b) exception

In practice, the requirements of Article 4 (1) (b) impose three conditions, all of which have to be fulfilled for the exception to public access to apply:

1. The privacy of the data subject must be at stake.
2. Public access must substantially affect the data subject
3. Public access is not allowed by the data protection legislation

1) Is the privacy of the data subject at stake?

The right to privacy, as defined in Article 8 of the European Convention on Human Rights, goes beyond the protection of private life in a strict sense - it may also include aspects of professional life - but is not endless. There must be a qualified interest of a person involved - the document must contain details about a person that are normally regarded as "personal" or "private". The mere fact that a document contains personal data of a general character, like the name of a person, should (normally) not hinder disclosure. In general, the privacy of the data subject is at stake if the document in question:

- contains sensitive data (such as data concerning health);
- concerns the honour and reputation of a person;
- could place a person in a false light;
- would disclose embarrassing facts;
- would disclose information given or received by the individual confidentially.

It should be noted that employees in a public administration are subject to a degree of public interest - for reasons of transparency and accountability - which is different from working in the private sector. One must keep in mind that it is not the employee in his or her personal capacity that attends, for example, a working group meeting at the Council - he or she is there in a public capacity, representing a Member State or one of the EU-institutions or bodies.

Therefore, some more general personal data, which are registered in the professional function of an employee of a public body, may fall outside the scope of the protection of privacy. This is even more obvious for high level staff, when they represent an EU-institution or body. These personal data might - also in those situations - still be subject to the Data Protection Regulation.

2) Is the data subject substantially affected?
For the data subject to be substantially affected by disclosure, there must be a degree of factual harm to his or her privacy. The public should not be deprived of their right to access if the privacy of the data subject would only be superficially affected. In quite a few situations, public access to a document does not affect the privacy of the data subject. Such would be the case, for instance, if the personal data concerned already has been made public at an earlier occasion.

In cases where it is likely that the privacy of the data subject could be substantially affected by disclosure, it is advisable to ask for the opinion of the data subject before deciding on it.

3) Is disclosure in accordance with data protection legislation?
When analysing the extent to which disclosure is allowed by data protection legislation, the principle of the right to information and the principle of proportionality play a key role.

3.1 The principle of the right to information

> As any exception must be interpreted and applied strictly, the Article 4 (1) (b) exception of the Public Access Regulation may only be applied insofar as the Data Protection Regulation explicitly prohibits disclosure of the personal data.

The Data Protection Regulation sets a number of conditions for the disclosure of personal data, the most important of which are mentioned here.

Disclosure of personal data must be compatible with the purposes for which they were collected (as decided at the time of the collection). If these purposes excluded disclosure to third parties -either explicitly or implicitly - then disclosure would infringe Article 4 of the Data Protection Regulation. In this context, the reasonable expectations of the data subjects would need to be taken into account.

Moreover, there are very restricted possibilities for disclosure of sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life (see Article 10).

Article 5 of the Data Protection Regulation allows disclosure if it is necessary for the performance of a task carried out in the public interest or in the legitimate exercise of official authority, or if it is necessary for the compliance with a legal obligation. On the one hand, this provision facilitates public access, if necessary to comply with the Public Access Regulation. On the other hand, this provision limits public access, since it does not allow for illegal or disproportionate disclosure of personal data - Article 5 should be regarded as the counterpart of Article 4 (1) (b), since the term 'necessary' requires a proportionality test.

3.2 The principle of proportionality

> The proportionality test consists of two elements:
> 1. Derogations to public access should remain within the limits of what is appropriate and necessary for achieving the aim in view (Court of Justice in the Council vs. Hautala case).
> 2. The test whether the same result could not be achieved by other less restrictive measures, for instance by giving partial access to the documents.

Firstly, it has to be analysed to what extent the rights of the data subject as safeguarded by the Data Protection Regulation are affected. In other words: what kind of harm does disclosure do to the data subject? In no case can the result of disclosure be that a person will be deprived - or unduly restricted in the exercise - of his (fundamental) right to data protection. The analysis will have to take into account:

- the kind of personal data processed;
- the compulsory or voluntary basis of the original collection of personal data;
- the situation of the data subject and the potential consequences of public disclosure;
- that disclosure causes less harm to the data subject if the document is handed over upon request than if it would be published on the Internet.

Secondly, if the unlimited disclosure of a document would have as a result that a private person is deprived of - or unduly restricted in - his fundamental right to data protection, less restrictive measures have to be taken into consideration. Partial access should be considered, for instance by erasing personal data before handing over the document to a third party. Certain passages or data in a document should be removed, unless it would result in an unreasonable amount of administrative work.

Three examples of Article 4 (1) (b) from the EU-institutions

The following examples are taken from a larger collection in the full text version of the paper. The first example is a 'proactive' case (general measure at early stage), while the second is 'reactive' (complaint with EDPS) and the third concerns a case in which public access could not be granted. The examples are simplified to fit the format of this brochure. The analyses follow the check-list in Chapter 6 of the paper.

Example 1: The European Ombudsman complaint form

The complaint form of the European Ombudsman informs the complainant of the consequences of a choice between public and confidential treatment. The complainant is therefore informed by the Ombudsman - in advance - of the possibility of public access.

Comment:

Is the privacy of the data subject at stake? Is he/she substantially affected by disclosure?

Arguably, the information given by a complainant or received from others may in many cases relate closely to their privacy. It is reasonable to expect that if the complainant chooses confidential treatment, his or her legitimate interests may be seriously affected by disclosure. Career or employment prospects could for instance suffer irrespectively of the outcome of the investigations of the Ombudsman.

Is disclosure allowed according to data protection legislation?

Through the form, the complainant is satisfactorily informed of the consequences of the choice between public and confidential treatment. In this context, 'unambiguous consent' for disclosure is obtained, in accordance with Article 2 (h) and 5 (d) of the Data Protection Regulation, should the complainant not request confidentiality. However, full public disclosure of documents concerning a complaint, where the complainant has opted for confidentiality, would breach Article 4, as it would go against the principle that the purposes are determined at the time of collection - as they could be reasonably understood by the data subject. In such cases, an anonymous version of a decision can still be published.

Example 2: The list of accredited assistants to the European Parliament may reveal the political opinion of an assistant - should it still be made public?

The list 'Assistants accredited to the European Parliament' contains the assistants of the MEPs. It lists them with their assistants, and as many of the assistants are likely to share the values of the Member they work for, the list may indirectly reveal their political opinion. The list is accessible from the website of the European Parliament and the names can be found with the internet search engine Google. Assistants can be excluded from the published list, as an exception, if they provide compelling legitimate grounds on how their privacy is infringed.

Comment:

Is the privacy of the data subject at stake? Is he/she substantially affected by disclosure?

The political opinion of a data subject is categorised as sensitive data and is intrinsically linked to the privacy of an individual. This type of information should in general not be disclosed. However, in situations like the one at hand there may be good reasons for doing so. It is hard to argue that assistants in general would be substantially affected by disclosure. The fact that it becomes public that someone works as an assistant for a MEP, and that he or she may share the values of the MEP, does not necessarily harm him or her. However, in specific cases (such as more extremist parties), disclosure could substantially harm the data subject, e.g. in a search for subsequent employment.

Is disclosure allowed according to data protection legislation?

The publication of the name of a person on the list of accredited assistants conforms with Article 4 of the Data Protection Regulation if it corresponds to the reasonable expectations of the data subject. There is a high degree of public interest in a parliament operating in a transparent way and disclosure is therefore in compliance with Article 5. Article 10 prohibits the processing of personal data revealing political opinions.

However, this provision is not absolute - important exceptions are laid down in Articles 10 (2) and (4).

Example 3: Can a list of trainees at an institution be made public?
In the case of a list of people who accepted a traineeship at an institution (the example originates from the European Parliament), public access has been refused on the grounds that it would breach the privacy of the trainees. When signing the application form, the applicant declares that he or she has read the 'Internal rules governing traineeships and study visits in the secretariat of the European Parliament'. Article 6.6 of those rules concerns the admission procedure and states: 'the results of the selection procedure will not be published'.

Comment:
Is the privacy of the data subject at stake? Is he/she substantially affected by disclosure?
In general, disclosure of information such as the names of people who most often have just completed university studies, and who have accepted a traineeship at a public body (such as a parliament), involves little privacy. In few cases would the data subject be harmed or substantially affected by disclosure. Applicants should however be given a possibility to opt-out on compelling and legitimate grounds.

Is disclosure allowed according to data protection legislation?
Although the names were collected for specific, explicit and legitimate purposes, in accordance with Article 4, it is imperative to keep in mind that the candidates were explicitly informed that their personal data would not be revealed. Disclosure would therefore run contrary to the reasonable expectations of the data subjects and - in spite of the strong case for public access (notably for reasons of accountability) - public access cannot be granted.

Conclusion

The paper deals with two fundamental rights - the right to public access, and the right to protection of personal data. These rights most often do not interfere with each other, but there are cases in which the two relevant Regulations apply simultaneously: the Article 4 (1) (b) exception. This provision contains a number of conditions which require a further examination.

A proper handling of requests for documents containing personal data is an important aspect of good governance. Therefore, the EU institutions and bodies must conduct a concrete and individual examination of each case, bearing the principles of the right to information and proportionality in mind. Compliance with both rights can be enhanced by proactive work, informing the data subjects properly in advance of how personal data will be dealt with - in full respect for the relevant Regulations.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail: edps@edps.eu.int
www.edps.eu.int
Tel.: 02-283 19 00 - Fax: 02-283 19 50

Printed in Belgium