EDPS - European Data Protection Supervisor

Public access to documents and data protection

Background Paper Series

July 2005

n°1

Public access to documents and data protection

© European Communities, 2005
Reproduction authorised for non-commercial purposes, provided the source is acknowledged.
Printed in Belgium

Table of contents

1. Introduction

This paper is on the relationship between public access to documents on the one hand and privacy, integrity and data protection on the other hand. It reflects the opinion of the European Data Protection Supervisor (EDPS) on this matter.

Public access to documents as well as privacy, integrity and data protection have been recognized as fundamental rights. Citizens of the European Union, nationals of third countries residing on the territory of a Member State and, in some cases, other nationals of third countries, are entitled to enjoy both rights. An adequate protection of both rights is needed because they are recognised not only as fundamental rights, but also as being elements of the notion of good governance. High levels of transparency and data protection are an expression of good governance.

As will be shown in the paper, the rights are of an extended character; both in terms of scope and of beneficiaries. These rights are deeply rooted in the constitutional traditions common to the Member States, and may be derived from various sources, be it Conventions of the Council of Europe, the EC and EU treaties or case law from the Court of Justice of the European Communities *(hereinafter: The Court of Justice)* or the European Court of Human Rights.

The application of these rights to the institutions and bodies of the European Communities is *inter alia* guaranteed by two Community regulations:

- Regulation (EC) No 45/2001 of the European Parliament and of the Council 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 data[1]. *This regulation will be referred to as 'data protection-regulation' or 'Regulation 45/2001'.*

- Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents[2]. *This regulation will be referred to as 'public access-regulation' or 'Regulation 1049/2001'.*

One should keep in mind that there is no hierarchical order between the two rights. Most often, as has been shown in statistics regarding the implementation of the public access regulation, there is no tension between the rights, even not in situations when both rights can be invoked at the same time.

However, in some cases the rights may collide, as the objective of the rules on public access is to foster access to all documents under the jurisdiction of the EU-institutions and bodies, whereas the data protection regulation must guarantee the protection of personal data. Examples of collision may be found in the administration of employment procedures, requests for information on employees of the institutions, information on participation in meetings organised by one of the institutions as well as in complaint procedures.

[1] OJ L 8, 12.01.2001, p. 1.
[2] OJ L 145, 31.05.2001 p. 43.

To illustrate the issue, a reference can be made to an Opinion of 17 May 2001[3] of the Article 29 Data Protection Working Party[4], in which it was underlined that 'personal data contained in an 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'. The opinion continues: '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 [...]'. The provisions of the relevant legislation on data protection therefore need to be respected.

As the examples that will be presented in this paper will show, the issue is of a general nature. This paper strives to address the issue in a practical, pragmatical and informative manner. It is not self-evident how the responsible Community-authorities should act if the two fundamental rights apply at the same time and one has to reflect clearly about which of the fundamental rights should be predominant in a particular case. This paper therefore strives to provide guidelines on how to interpret the relevant community legislation, when considering publishing a document which contains personal data, when dealing with a request for access to such a document or when dealing with a complaint about the disclosure of a document.

The aim of this paper is threefold. Firstly, it is to show that public access to documents and data protection shall not be seen as contrary, but complementary, to each other. Secondly, it is to identify areas of tension. Thirdly, it is to promote good practice within the institutions and bodies of the EU. Good practice in this sense involves *inter alia*:

1. An institution or a body should consider whether rendering partial access to a document - by deleting (direct and indirect) references to persons - could take away the conflict between the two fundamental rights.
2. An institution or a body should consider adopting internal rules on the access to *certain* documents containing personal data (the proactive approach), or at least inform the data subject in advance about the way the data will be used.

The paper is structured as follows:

- Chapter 2 focuses on transparency, notably public access. This involves, *inter alia*, a definition, a description of the legal history and background and a thorough examination of the public access regulation.
- Chapter 3 focuses on privacy and data protection, and is structured similarly to chapter 2.
- Chapter 4 explores the intersection of the two fundamental rights. This involves, *inter alia*, some guiding principles. This chapter contains the key element of this paper: the analysis on the exception to public access, included in Article 4 (1) (b) of the public access regulation.
- Chapter 5 elaborates some experiences with the issue within the institutions.
- Chapter 6 contains a checklist which aims to guide the reader in cases where the two rights may collide.

[3] Opinion 5/2001; http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp44en.pdf. The Opinion was given in the context of a complaint to the European Ombudsman in a case [T-194/04 Bavarian Lager v European Commission] which is now pending before the Court of First Instance (see also example 9).
[4] This is an independent advisory group, composed of representatives of the data protection authorities of the Member States, the EDPS and the Commission, which was set up by Directive 95/46/EC.

2. Transparency and public access

2.1. Definition

Transparency, or as it is sometimes called, openness, "enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system. Openness contributes to strengthening the principles of democracy and respect for fundamental rights as laid down in Article 6 of the EU Treaty and in the Charter of Fundamental Rights of the European Union."[5] In its case law, the Court of Justice has repeatedly stressed the close link with the democratic nature of the institutions.[6]

Transparency generally involves three elements:

1. the processes through which public bodies make decisions should be understandable and open;
2. the decisions themselves should be reasoned;
3. as far as possible, the information on which decisions are based should be available to the public.

This chapter will mainly deal with the third element of transparency: the public access to information on which decisions are based or, even more concretely, to documents of the institutions. The right of access to these documents is - as far as the European Parliament, the Council and the Commission are concerned - guaranteed in Regulation 1049/2001. Article 4 (1) (b) of this regulation is the entry point for the assessment of the interference between public access and data protection and will play a central role in this paper.

2.2. Legal history and background

During the last decade of the last century, the lack of transparency in the Community institutions was high on the political agenda. Amongst many initiatives taken in the general context of openness, several efforts aimed at improving the public's right of access to documents.

The first real step towards allowing the public a right of access to EC-documents was taken in February 1992, when the Member States signed the final act to the Maastricht Treaty. In Declaration 17, attached to the Maastricht Treaty, it was stated that transparency of the decision-making process would strengthen the democratic nature of the institutions and the public's confidence in the administration. Accordingly, it was recommended that the Commission submit to the Council a report on measures designed to improve public access to the information available to the institutions.

Following the signing of the Maastricht Treaty, a series of political developments forced the European politicians into action in the field of transparency: The Danish voters said no to the Maastricht Treaty, in France only a very narrow majority supported this treaty and in several

[5] Quotation of the second recital of the public access regulation.
[6] See, for instance, Case C-58/94 Netherlands v Council [1996] ECR I-2169.

other Member States, the enthusiasm for the European idea declined. A number of initiatives were taken. In the so-called Birmingham Declaration[7] on 'A Community closer to its citizens', the Council engaged itself to more openness in the decision-making process. The Commission carried out a survey of national laws and practices. In 1993, the Council and the Commission jointly adopted a code of conduct on public access to documents[8], which was implemented shortly thereafter[9]. Subsequently, at the request of the European Ombudsman, other Community institutions and agencies have introduced rules on access to documents[10].

2.3. The legal basis for EU-level action

The notions of openness and access to documents were introduced into the Treaties by the adoption of the Treaty of Amsterdam. Article 1 (2) EU provides that decisions shall be taken 'as openly as possible'. A new Article 255 inserted into the EC-Treaty established the right of access to 'European Parliament, Council and Commission documents'. Article 255 (2) established that the content of this right as well as its exceptions should be laid down in secondary EC-legislation.

Article 255

1. *Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, shall have a right of access to European Parliament, Council and Commission documents, [...].*
2. *General principles and limits on grounds of public or private interest governing this right of access to documents shall be determined by the Council, acting in accordance with the procedure referred to in Article 251 within two years of the entry into force of the Treaty of Amsterdam.*
3. *Each institution referred to above shall elaborate in its own Rules of Procedure specific provisions regarding access to its documents.*

By enacting Regulation 1049/2001, the European Parliament and the Council have implemented the provisions of Article 255 of the EC Treaty. The legal basis does not extend to other institutions and bodies than the three mentioned in Article 255. Aware of this shortcoming, the Council made the executive agencies to be entrusted with certain tasks in the management of Community programmes subject to Regulation 1049/2001[11]. Prior to that, the European Parliament, the Commission and the Council adopted a joint declaration[12] in which they:

---

[7] See the so-called Birmingham Declaration, Annex 1 in Bulletin of the European Communities, n°10, 1992.
[8] Council and Commission Code of Conduct concerning public access, OJ L 340, 31.12.1993, p.41.
[9] Decision 93/731/EC of the Council of 20 September 1993 on Public Access to Council Documents (OJ L 340, 31.12.1993, p.43) and Decision 94/90/ECSC, EC, Euratom of 8 February 1994 of the Commission on Public Access to Commission Documents (OJ L 46, 18.02.1994, p. 58).
[10] Special report of 15 December 1997 by the European Ombudsman to the European Parliament following the own initiative inquiry into public access to documents (616/PUBAC/F/IJH), see: http://www.euro-ombudsman.eu.int/special/en/default.htm. The EDPS will respect the provisions of the public access regulation; this will be established in the rules of procedure.
[11] Council Regulation (EC) No 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes (OJ L 11, 16.01.03, p. 11)
[12] OJ L 173, 27.06.2001, p.5.

1. undertake to make the regulation applicable to agencies and similar bodies set up by the Community legislator;

2. appeal to the other institutions and bodies to adopt similar rules voluntarily.

Most other institutions and bodies have modified their internal rules with the result that they now include the same elements as Regulation 1049/2001. For example, the European Central Bank (ECB), in its Decision of 4 March 2004 on public access to ECB documents, makes an explicit reference to the joint declaration referred to above.

2.4. The public access regulation

2.4.1. General provisions

On 30 May 2001, Regulation 1049/2001 was adopted. This regulation was preceded by some 18 months of complicated negotiations. The purpose of the regulation is threefold: to define the principles, conditions and limits governing the right of access to documents; to establish rules ensuring the exercise of this right and to promote good administrative practice (Article 1).

The right of access to documents is defined in Article 2 (1) of the regulation.

> ***Article 2(1)***
>
> *Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, has a right of access to documents of the institutions, subject to the principles, conditions and limits defined in this Regulation.*

The scope of the regulation *ratione personae* is wide, but the right of access extends even further, as the institutions may grant access to any natural or legal person not residing or not having its registered office in a Member State.

Public access applies to all documents held by an institution, that is to say, documents drawn up or received by it and in its possession, 'in all areas of the activity of the European Union', so not only in activities under Community law (the 'first pillar'). This means that the regulation expressly applies in the second and third pillar.

The term document is defined broadly so as to include any content, whatever its storage medium, concerning a matter relating to the policies, activities and decisions falling within the institution's sphere of responsibility (Article 3).

The regulation provides a two-stage administrative procedure for application, followed by the possibility to contest a refusal through court proceedings or complaint to the European Ombudsman.

Finally, one should keep in mind that the principle of access in essence consists of:
- the right to information contained in public documents as well as,
- the right of access to the documents themselves.

This remark is important since it means that a Community institution may - if an exception to public access applies - consider giving partial access to a document. In certain circumstances, an institution might even be obliged to do so[13].

2.4.2. The nature of the right of access to documents

The right of access to documents must be read and interpreted in accordance with the case law of the Court of First Instance, based on legislation that preceded Regulation 1049/2001, notably Council Decision 93/731 and Commission Decision 94/90. In Svenska Journalistförbundet vs. Council[14], the Court of First Instance stated: "The objective of Decision 93/731 on public access to Council documents is to give effect to the principle of the largest possible access for citizens to information with a view to strengthening the democratic character of the institutions and the trust of the public in the administration. It does not require that members of the public must put forward reasons for seeking access to requested documents."

The right of access thus comprises the following essential elements:

- It is a right for any member of the public.
- It not relevant for what reason someone wants to exercise his right.

The notion 'any member of the public' is a very wide notion, as has been shown in the preceding paragraph. Moreover, this notion includes a second characteristic: it confers the same right to every member of the public. Article 2 of Regulation 1049/2001 does not recognise privileged groups of persons to whom - for instance - the exceptions to the right of access do not fully apply, like for instance members of a parliament, journalists, or - specifically related to the subject of this paper - 'data subjects', or members of the staff of an institution.

In short, it is not relevant in what capacity someone asks for the disclosure of a public document. Under Community law, additional rights of access to public documents for privileged groups follow from separate legal provisions that can be seen as a 'lex specialis' in relation to Article 2 of Regulation 1049/2001.

The data subject who him- or herself asks for access to documents, containing his or her personal data, can base the request to a community institution or body either on Article 2 of Regulation 1049/2001 or on Article 13 of Regulation 45/2001. Article 13 of the data protection regulation 45/2001 could give the data subject a stronger right to access to such documents, since the exceptions to the public access regulation do not apply as such. This paper will not elaborate on the situation in which the data subject asks for access to documents. The right of access of the data subject is a part of the principles of data protection and has nothing to do with the transparency and the accountability of a public body.

Special provisions on the access to information of the institutions can further be found in the Staff Regulations. Article 26 provides for access of a staff member to his own personal file and will not be elaborated in this paper. However, Article 25 (3) of the Staff Regulations

[13] See the Judgment of the Court of Justice in Council vs. Hautala, elaborated in Pars. 2.4.3 and 4.2.
[14] Judgment of the Court of First Instance Svenska Journalistförbundet v Council, T-174/95, ECR [1998], p. II-2289. See also: Judgment of the Court of First Instance, Interporc v Commission, T-124/96, ECR [1998] Page II-231.

introduces special rules to guarantee the transparency of certain decisions of the Authority that appoints staff members. It states:

> Specific decisions regarding appointment, establishment, promotion, transfer, determination of administrative status and termination of service of an official shall be published in the institution to which the official belongs. The publication shall be accessible to all staff for an appropriate period of time.

It is obvious that these decisions contain personal data and are highly relevant within the framework of this paper. A staff member has a right of access to these data, on the basis of this provision, regardless of the right of access guaranteed by Regulation 1049/2001; the exceptions to public access of this regulation do not apply.

Hereinabove we mentioned a second essential element: it is not relevant either for what reason someone asks for the disclosure of a public document. The authority that decides on the public access of a certain document is not allowed to take into account why someone asks for access, nor is it allowed to weigh the importance of access to the person involved. Any other interpretation would seriously impede the main objectives of Article 2 of Regulation 1049/2001, as has been interpreted by the Court of First Instance.

2.4.3. The exceptions

Article 4 contains the categories of exceptions to public access.

> **Article 4 (1)**
>
> *1. The institutions shall refuse access to a document where disclosure would undermine the protection of:*
>
> *(a) the public interest as regards:*
> *– public security,*
> *– defence and military matters,*
> *– international relations,*
> *– the financial, monetary or economic policy of the Community or a Member State*
>
> *(b) the privacy and integrity of the individual, in particular in accordance with community legislation regarding the protection of personal data.*

The exceptions of Article 4 (1) have a general scope and are formulated compulsory and absolute. In a report from the Commission on the implementation of the regulation it is stated: 'should disclosure of a document cause harm to one of the interests mentioned, access to this document should be denied'[15]. As has been mentioned before, Article 4 (1) (b) will play a central role throughout this paper. This provision will be explained more in depth in paragraphs 2.4.3 and 4.3.

[15] Report from the Commission on the implementation of the principles in EC Regulation n° 1049/2001, COM (2004)45 final, p.17.

By contrast with the exceptions under Article 4 (1), the exceptions provided for by Article 4 (2) and 4 (3) have a more limited scope. Both exceptions are subject to an overriding public interest in disclosure. This implies a balancing of the public interest in disclosure against the protection of another interest.

Article 4 (2) and 4 (3)

2. The institutions shall refuse access to a document where disclosure would undermine the protection of:

— commercial interests of a natural or legal person, including intellectual property,

— court proceedings and legal advice,

— the purpose of inspections, investigations and audits,

unless there is an overriding public interest in disclosure.

3. Access to a document, drawn up by an institution for internal use or received by an institution, which related to a matter where the decision has not been taken by the institution, shall be refused if disclosure of the document would seriously undermine the institution's decision making process, unless there is an overriding public interest in disclosure.

Access to a document containing opinions for internal use as part of deliberations and preliminary consultations within the institution concerned shall be refused even after the decision has been taken if disclosure would seriously undermine the institution's decision making process, unless there is an overriding public interest in disclosure.

Article 4 (3) is intended to protect the so-called space-to-think. The regulation makes a distinction between cases where the institution has not yet finished its thinking and those where the thinking period is over because the institution has made a decision.

As regards third-party documents, the institution shall according to Article 4 (4), consult the third party with a view to assessing whether one of the exceptions is applicable. A Member State may request the institution not to disclose a document originating from that Member State without its prior agreement (Article 4 (5)). In case a Member State holds a document originating from an institution, it is according to Article 5 entitled to apply its own national law on public access.

Article 4 (6) states that if only parts of the requested document are covered by any of the exceptions, the remaining parts of the document shall be released - partial access. This is an important element, as it restricts the scope of exceptions to only cover the specifically excepted information of a particular document (see also 4.2.3).

Finally, Article 9 contains a set of special provisions as regards sensitive documents. These documents (called EU RESTRICTED) are classified with "Top Secret", "Secret" or "Confidential" in accordance with the security rules of the institution concerned. They protect essential interests of the EU or one or more of its member states in the areas covered by Article 4 (1) (a), notably public security, defence and military matters.

2.4.4. The exception of Article 4 (1) (b)

As has been stated in the previous paragraph, the exceptions of Article 4 (1) are formulated compulsory and absolute. However, despite this legal and absolute appearance, these exceptions should not be applied mechanically, as has been demonstrated by the case-law of the Court of Justice - in particular the Council vs. Hautala-case[16]- and supported by several policy documents[17]. According to the Court of Justice, exceptions to a fundamental right such as Article 4 (1) (b) should be construed and applied strictly, in a manner which does not defeat the application of the fundamental right. Furthermore, the principle of proportionality requires that derogations remain within the limits of what is appropriate and necessary for achieving the aim in view.[18]

This leads to the elements of Article 4 (1) (b). This provision must be analysed on a case-by-case basis, where three elements need to be taken into account:

1. The terms 'privacy and integrity' will be further explored in the next chapter. It is clear that the wording calls for an interpretation of circumstances, given the fact that the same data being revealed in different circumstances can lead to different conclusions as to whether or not someone's privacy and integrity have been affected. The mere fact that a document mentions personal data does not automatically mean that the privacy and integrity of a person are affected.
   Summarized: the privacy and the integrity of the data subject must be at stake.

2. The words 'would undermine' imply that the protection of the privacy and integrity of an individual must be harmed. The level of harm needed for the applicability of the exception to public access is not mentioned. However, the wording 'undermining' implies that the effect on the interest of the data subject should be substantial. It has to be added that the conditions for applying the exception of Article 4 (3) seem to be more strict. Disclosure must "seriously undermine" the decision-making procedure. However, the distinction between undermining and seriously undermining is very theoretical and will not be considered to be important for the purpose of this paper.
   Summarized: public access must substantially affect the data subject.

3. The harm done to a person's privacy and integrity should be examined 'in accordance with community legislation regarding the protection of personal data'. The prime sources of community legislation regarding the protection of personal data are Directive 95/46/EC and Regulation (EC) 45/2001. Both legal instruments will be discussed in the following chapter of this paper.
   Summarized: public access can only be given if this is allowed by the data protection legislation.

The document that is requested may in some cases fall outside of the scope of Regulation 45/2001 because it does not correspond to the requirements laid down in its Article 3. This, however, does not mean that the analysis of the 4 (1) (b) exception to Regulation 1049/2001 does not have to take the general principles of protection of personal data in consideration. In

[16] Judgment of the Court, Council of the European Union v Heidi Hautala, C-353/99 P, ECR [2001] p. I-9565.
[17] See more in detail Paragraph 4.2.
[18] See paragraphs 84-85 of the Judgment of the Court of First Instance in the Hautala-Case, quoted in paragraph 8 of the Judgment of the Court (C-353/99 P).

other words: also under such circumstances, one needs to examine whether the privacy of an individual will be substantially affected (elements 1 and 2).

2.5. Implementation of the public access regulation

The European Parliament, the Commission and the Council have each laid down specific provisions regarding access to its documents in their rules of procedure and in additional measures. For example, the Council adopted a range of documents which, apart from the rules of procedure, concern *inter alia* a decision on making certain categories of documents available, a decision on the protection of classified information and a decision on the improvement of information on the legislative activities of the Council. Moreover, most EU institutions and bodies have laid down provisions regarding access to their documents in their rules of procedure (see paragraph 2.2).

According to Article 17 of the public access regulation, each institution shall annually publish a report for the preceding year, including the number of cases in which the institution refused to grant access to documents, the reasons for such refusals and the number of sensitive documents not recorded in the registers[19].

In January 2004, the Commission issued its first report on the implementation of the principles in the public access regulation. It shows that the voluntary arrangements of public access often fall short of the rules in the regulation[20]. The report also shows that full access was given to some 76 and 62 per cent respectively of the Council and the Commission documents. The corresponding figures for partial access were 12 and 8 per cent. At the same time the European Parliament refused access to 9 out of 528 admissible applications. The statistics of the report show furthermore that only in a small number of applications for access to documents the exception of Article 4 (1) (b) plays a role.

As the figures are composed in different ways in the different institutions, they can only be used as an indication of how refusals to publish a document are founded. The figures should therefore not be subject to extensive analysis. However, what is clear is that the exception on the ground of privacy and integrity of the individual is not the most frequently used exception. In the Council, access to documents is mainly refused for reasons of public security and international relations. The Commission denies access mainly for reasons of inspection, investigation or audit.

2.6. The Charter of Fundamental Rights and the Constitution

Although the Treaty establishing a Constitution for Europe (*hereinafter Constitution*) has not been ratified by the Member States[21], it provides a useful reference to the current thinking in the fields of transparency, data protection and privacy. Part II of the Constitution incorporates the Charter of Fundamental Rights, which was signed and proclaimed by the Presidents of the European Parliament, the Council and the Commission at the European Council meeting in

[19] Note by the Secretary-General of the EP to the bureau, dated 23 January 2003 (PE 324.892/BUR); Report from the Council, dated 31 March 2003 (7957/03) and Report from the Commission, dated 29 April 2003 (COM (2003) 216 final).
[20] Report from the Commission on the implementation of the principles in EC Regulation 1049/2001; COM (2004) 45 final, p.16.
[21] At the dateof the finalization of the paper, 14 June 2005.

Nice on 7 December 2000. According to Article I-9, the European Union shall recognise the rights, freedoms and principles set out in the Charter of Fundamental Rights of the Union.

In the Constitution, the principles of openness and access to documents are incorporated in three different articles. The general principle of openness is embodied in Article I-50 of Title VI - 'The democratic life of the Union'. This article, entitled 'Transparency of the proceedings of Union institutions', promotes good governance, participation of the civil society and open meetings. It explicitly refers to the right of access to documents to the Union institutions, bodies, offices and agencies and thus deals with the discrepancy between the current legal base and the reality. Moreover, the text of paragraph 3 refers to Article 399 in part III - 'The Union's policies' - of the Constitution, which lays down the conditions under which the right to access to documents of the European institutions is guaranteed.

Article II-102, that has already been recognised in the existing Charter of Fundamental Rights of the Union, closely resembles Article 255 of the EC Treaty and repeats once again the right of access to documents.

The Constitution lays down that all institutions, bodies and agencies of the EU shall recognise the importance of transparency, including the Court of Justice and the European Central bank, when exercising their administrative tasks.

3. 'Privacy and integrity' and 'data protection'

3.1. Introduction

'Privacy', 'integrity' and 'data protection' are all notions with a history longer than that of transparency in the Member States and on the wider European level. Respect for the private life has been ensured on the European scale since the adoption in 1950 by the Council of Europe of the Convention for the Protection of Human Rights and Fundamental Freedoms (*hereinafter European Convention on Human Rights*). Due to technical developments, it was necessary to enlarge the scope and refine the terms. Other legislative instruments saw the day, such as the European Convention for the protection of individuals with regard to the automatic processing of personal data, which was adopted in 1981 (*hereinafter Convention 108*)[22]. Today, at the EU-level, the basic rules on data protection are laid down in:
- 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[23];
- Regulation (EC) No 45/2001 of the European Parliament and of the Council 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 data (the *'data protection-regulation;* see Ch. 1).
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[24].

It is good to bear in mind - and this will be discussed more in detail - that the concepts of 'privacy and integrity' on the one side and 'data protection' on the other side are not identical. The protection of privacy is a fundamental right that is primarily protected by Article 8 European Convention on Human Rights and subsequent provisions within the framework of the European Union. The concept of protection of personal data contains basic principles to protect the data subject. On the one hand, the concept of data protection is narrower than privacy since privacy encompasses more than personal data. On the other hand, it encompasses a wider area, since personal data are protected not only to enhance the privacy of the subject but also to guarantee other fundamental rights, such as the right not to be discriminated.

As has been shown in Chapter 2, a general understanding of the data protection legislation is necessary, not only for processing of personal data, but also for understanding how to interpret Article 4 (1) (b) of the public access regulation. This chapter explores the legislative history and background and lifts out important elements of the data protection regulation.

Finally, the Article 29 Data Protection Working Party stated that the status of the personal data does not change, just because they are part of an official document[25]. In the same opinion, the Working Party also underlines the fact that while regulating processing of

[22] http://conventions.coe.int/treaty/en/Treaties/Html/108.htm
[23] OJ L 281, 23.11.1995, p. 31.
[24] OJ L 201, 31.07.2002, p. 37.
[25] In Opinion 5/2001, referred to in the introduction.

personal data, the data protection regulation itself also opens up the possibility for making personal data public.

3.2. Legal history and background

3.2.1. The concepts of privacy and integrity

In a UNESCO document of 1994, privacy was considered to be perhaps the most difficult to define of all human rights, yet nearly every country in the world has included a right of privacy in its constitution[26]. As a matter of fact, the definitions vary according to context as well as to environment.

If one nevertheless looks for a description, one could indicate that privacy protection is frequently seen as a way of drawing the line as to how far the society can intrude into a person's affairs. A still relevant description has been given in a Resolution, adopted by the Parliamentary Assembly of the Council of Europe, already in 1970:

"The right to privacy consists essentially in the right to live one's own life with a minimum of interference. It concerns private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially."[27]

Privacy is in that sense a private sphere exempted from disclosure, which allows the individual to remain in a feeling of control over himself and the surrounding environment close to him. According to case law of the European Court of Human Rights, privacy extends to the workplace. It thus follows that the reputation and the professional integrity of an individual forms an integral part of the notion of privacy[28]. As such, it is intrinsically linked to the term integrity.

The term integrity is also difficult to define. It can be seen as a fundamental right of a person to live according to his values and not to be affected. Integrity lies close to human dignity. Integrity is a right which is not absolute, as a modern society would not function if no one could interfere in another person's life and values. One thus needs to find a balance between total integrity and total lack of integrity.

In the context of public access to documents and data protection the term 'integrity' does not add much to privacy. It is not easy to conceive how disclosure of personal data could harm a person's integrity but not his privacy. Maybe, one could envisage the exceptional situation when disclosure of data would endanger the physical integrity of a person (if he is threatened, for instance). It is in the light of this that the 'privacy and integrity' exception of the public access regulation has to be seen.

[26] EPIC Privacy and Human Rights Report 2004, p.1.
[27] RESOLUTION 428 (1970), containing a declaration on mass communication media and human rights, published on http://assembly.coe.int/Documents/AdoptedText/ta70/ERES428.htm
[28] See also Par. 4.3.3

For reasons of simplicity, this paper, when looking into the intersection of the two fundamental interests of privacy and public access, will in hereafter refer to privacy and not to 'privacy and integrity'.

3.2.2. Protection of privacy

The European Convention on Human Rights of 1950 established a 'right to privacy'. Its Article 8 stipulates the 'Right to respect for private and family life'.

> 1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
> 2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Moreover, Article 7 of the Charter of the Fundamental Rights of the Union reads as follows.

> *Respect for private and family life*
> *Everyone has the right to respect for his or her private and family life, home and communications.*

According to the case law of the European Court of Human Rights, and subsequently of the Court of Justice and the Court of First Instance, the area covered by the term privacy is interpreted *sensu lato* (encompassing the protection of private life, but also extending beyond), rather than *sensu stricto* (private and family). The courts have thus clearly opted for a broad scope of the right of privacy which extends further than the notion of respect for private and family life of Article 7 of the Charter of Fundamental rights.

This interpretation has two consequences.
– In the first place: a connection with the respect for private and family life is needed. This means that normally the simple mentioning of a persons name and address does not qualify. However, this can be different if these data are placed in a specific context[29].
– In the second place: the European Court of Human Rights has clearly opted for a broad scope of the right of privacy, by stating that the notion "private life" may cover private, business, public or any other environment.

This broad scope was established in the Niemietz case[30]:

> *Respect for private life must also comprise to a certain degree the right to establish relationships with other human beings. It is after all, in the course of their working lives that the majority of people have significant if not the greatest opportunity of developing relationships with the outside world.*

[29] For instance, a specific context mentioned in the quoted text of the Resolution of the Parliamentary Assembly; see Par. 3.2.1.
[30] Judgment of 16 December 1992, A-251.B, point 33.

This principle was reaffirmed several times, *inter alia* in Amann[31].

> *The expression of the term private life must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; there appears to be no reason in principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature.*

In the Österreichischer Rundfunk and Others-case[32], the Court of Justice confirms that, as far as an act falls within the scope of Community Law, the term private life must not be interpreted restrictively.

3.2.3. Protection of personal data.

The protection of personal data has been guaranteed for the first time - as a separate right granted to an individual - in Convention 108.

Moreover, Article 8 of the Charter of the Fundamental Rights of the Union reads as follows.

> *Protection of personal data*
> *1. Everyone has the right to the protection of personal data concerning him or her.*
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
> *3. Compliance with these rules shall be subject to control by an independent authority.*

During the 1960's and 1970's, the potential impact of the developments in the field of information and communication technologies on the life of citizens became visible, for instance because of the increase of surveillance possibilities, both in the public and the private sector. Moreover, the existing legislation designed to secure the privacy of personal information was no longer felt to be adequate. The term 'private life' in the ECHR had a number of limitations in the light of these new developments. The scope was uncertain and the emphasis was on protection against interference by public authorities and not by private organisations.

Convention 108 was adopted in 1981. The Council of Europe responded in this way to the new developments in the area of information and communication technologies. At the same time, the Organization for Economic Co-operation and Development (OECD) had issued guidelines to its members which urged them to introduce measures to protect personal information.

The Convention offered a blueprint for the harmonisation of data protection in each signatory state, by seeking to enhance personal freedoms and enable the free movement of personal data between countries. Convention 108 did not directly confer rights to European citizens; it was addressed solely to the Member States of the Council of Europe. Its main function was to encourage States without or with inadequate data protection to legislate in this field and to

[31] Judgment of 16 February 2000, Reports 2000-II
[32] Judgement cited in Footnote 34.

start a debate on the topic[33]. As the Convention allowed signatory states to exclude some categories of data from the scope of the Convention, this led to different levels of data protection, with the result that inconsistencies between national regulatory systems remained.

Thus, long before initiative was taken at Community level, most European countries had enacted legislation designed to balance the individual's right to data protection with the need of public authorities, employers and others to process data. These domestic laws were in many respects similar, since they were based on Convention 108.

The wording of the Convention 108, as well as the explanation given in the Convention's explanatory report, specifies that data protection does not only concern protecting privacy and family life, but also other rights and fundamental freedoms.

In Article 1, the objective and purpose of the Convention are defined:

> *The purpose of this Convention is to secure [...] for every individual [...] respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").*

The right to protection of personal data encompasses the protection of privacy, but extends beyond it. Data protection is about securing respect for rights and fundamental freedoms, and *in particular* (i.e. not only) the right of the data subject to privacy. This is further explained in the Convention's explanatory statement. Recital 25 states:

> *The preamble reaffirms the commitment of the signatory States to human rights and fundamental freedoms. Moreover, it acknowledges that the unfettered exercise of the freedom to process information may, under certain conditions, adversely affect the enjoyment of other fundamental rights (for example privacy, non-discrimination, fair trial) or other legitimate personal interests (for example employment, consumer credit). It is in order to maintain a just balance between the different rights and interests of individuals that the convention sets out certain conditions or restrictions with regard to the processing of information. No other motives could justify the rules which the Contracting States undertake to apply in this field.*

This interpretation is further confirmed by Article 3, in which it is stated that any State may give notice:

> *[...] that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality.*

[33] ZERDICK, T. "*European aspects of data protection, what rights for the citizen?*" in: Legal Issues of European Integration, nr. 2, 1995, p.64.

3.2.4. Protection of personal data in the framework of the EC-Treaty

The data protection directive

Despite Convention 108, too many inconsistencies between national regulatory systems remained. Such disparities seemed incompatible with the growth of the European Community and global information flows in the early nineties. In response to the growing pressure, a Community-wide approach to data protection was deemed necessary. In 1990, the Commission adopted a package of measures, aimed at securing a community-wide approach to data protection, developed to harmonise national provisions in this field. The main element was a proposal for a framework directive, which had two primary aims:

- to protect the fundamental rights and freedoms of natural persons and in particular their right of privacy with respect to the processing of personal data,
- to prevent barriers to the free flow of personal data across the Community.

The proposal was contested and the Commission had to revise it. However, at the same time, the political importance given to the harmonisation of data protection grew. In this sense, the Commission white paper 'Growth, competitiveness and employment - the challenges and ways forward into the 21st century', which acknowledged the irreversible shift towards an information society proved an important element. Directive 95/46/EC was adopted in 1995, following the submission to the European Council of the report 'Europe's way forward to the information society', by a high-level group on European information structures[34]. As a result, personal data of all citizens shall have equivalent protection across the EU. This protection was later also extended to the field of electronic communications.

The privacy and electronic communications directive

The privacy and electronic communications directive is based on the same principles as the data protection directive. The directive was adopted in 1997[35] and replaced in 2002 by an updated version: directive 2002/58 on privacy and electronic communications. The aim was to regulate areas that were not sufficiently covered by the data protection directive, such as access to billing data, marketing activities, etc. The 2002 directive reflects developments in the markets and technologies for electronic communication services, such as the Internet, so as to provide an equal level of protection of personal data and privacy, regardless of the technologies used[36].

The directive was part of a package of five directives and one decision intended to reform the existing regulatory framework for electronic communications services and networks in the Community. One of the aims of this overall reform was to create technologically neutral rules, i.e. ensuring that services are regulated in an equivalent manner, irrespective of the technological means by which they are delivered. This implied that consumers and users should get the same level of protection regardless of the technology used by a particular service.

[34] The group was led by Commissioner Bangemann.
[35] Directive 97/66, OJ L 24, 30.1.1998, p.1.
[36] COM(2003)265 final, p.4.

The interpretation of these Community instruments

Both directives must be interpreted in the light of fundamental rights. We quote the Court of Justice in the Österreichischer Rundfunk and Others-case[37]:

> *The provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures [...]. Those principles have been expressly restated in Article 6(2) EU, which states that `[t]he Union shall respect fundamental rights, as guaranteed by the [European Convention on Human Rights] and as they result from the constitutional traditions common to the Member States, as general principles of Community law.*

The Court of Justice refers expressly to the relevant Case law of the European Court of Human Rights.

3.2.5. Both rights are interrelated. The protection extends to public information.

Although the two fundamental rights - respect for privacy and protection of personal data, each with their own characteristics - are separately mentioned, one has to bear in mind, that both rights are closely connected and even overlap each other to a very high extent. This is a consequence of the *sensu lato* interpretation of privacy by the courts. In the Rotaru case[38], the European Court of Human Rights specifies:

> *Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities.*

Nevertheless, there are cases of processing of personal data that have no link to privacy. A clear cut example can be found in people being registered when performing a public role. One could think for instance of a Member of the European Parliament entering the premises of the Parliament and this being registered by the processors linked to the automatic gates. His or her data are processed, but there is no link to privacy.

It is useful in this context to refer once again to the Judgment in Österreichischer Rundfunk and Others. The Court dealt with an Austrian law providing for the transfer of salary details on public sector employees to the Austrian Court of Auditors and their subsequent publication. In its judgment the Court:

- lays down a number of criteria drawn from Article 8 of the European Convention on Human Rights, which should be applied when evaluating Directive 95/46/EC in so far as this directive provides for certain restrictions to the right to privacy (see 3.2.4);
- makes it clear that Directive 95/46 has a wide scope. The protection given by the Directive extends to the processing of personal data, even if there is no connection with the exercise of the right to privacy.

[37] Judgment of the Court of 20 May 2003, Joined cases C-465/00, C-138/01 and C-139/01. ECR 2003, Page I-4989, Paragraphs 68 and 69.

[38] Judgment of 4 May 2000, Reports 2000-V

3.3. The legal basis for EU-level action

3.3.1. Article 286 EC

Article 286 of the EC Treaty, adopted in 1997 as part of the Treaty of Amsterdam, provides that rules on the level of the EU institutions and bodies should be similar to the rules on the national level. This includes the establishment of an independent supervisory authority:

> *1. From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty.*
>
> *2. [...] the Council, acting in accordance with the procedure referred to in Article 251, shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate.*

3.3.2. The data protection regulation: introduction

In Regulation 45/2001 the European Parliament and the Council have implemented Article 286 of the EC-treaty. They have enacted the rules concerning 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 data. The data protection regulation provides for the establishment of the European Data Protection Supervisor[39]. The following section examines and highlights the most important elements of the Regulation, particularly with respect to the relationship with the public access regulation.

Similarly to both directives mentioned in Paragraph 3.2.4, the regulation must be interpreted in the light of fundamental rights, in so far as it deals with processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy.

3.4. The main elements of the data protection regulation

3.4.1. General provisions

Article 1 of the regulation sets out the objective, which is twofold:

- *for the institutions and bodies [...] to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and to neither restrict, nor prohibit the free flow of personal data between themselves or to recipients subject to [the principles of the data protection directive];*
- *to establish an independent supervisory authority to monitor the provisions of the*

[39] See also Decision 1247/2002/EC of the European Parliament, of the Council and of the Commission on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties, JO L 183, 12.7.2002, p. 1.

regulation to all processing operations carried out by a Community institution or body.

Article 2 lays down the definitions of the regulation:

- *'Personal Data' means any information relating to an identified or identifiable natural person, which is called 'Data subject';*
- *'Processing of personal data' means any operation or set of operations, which are 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, [...];*
- *'The data subject's consent' means any freely given specific and informed indication of his or her wishes by which the data subject signifies his agreement to personal data relating to him being processed.*
- *'Controller' means the unit or entity which determines the purposes and means of the processing.*

Disclosure of data - by transmission and dissemination or otherwise making available - falls within the definition of 'processing'. By mentioning disclosure as a way of processing, the data protection regulation it self, *nota bene*, independently of the public access regulation, creates the possibility of making personal data public.

Article 3 lays down the scope, and specifically states that the regulation applies to:

- *'all Community institutions and bodies' (criterion ratione personae)*
- *'in so far as the processing of personal data is carried out in the exercise of activities all or part of which fall within the scope of Community law' (criterion ratione materiae)*
- *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.*

The first indent, *Criterion ratione personae*, establishes more specifically that the regulation applies to the processing of data by the institutions: the European Parliament, the Council of the European Union, the European Commission, the Court of Justice and the Court of Auditors. Moreover, it applies to: the European Central Bank, the European Investment Bank, the Ombudsman, the Economic and Social Committee and the Committee of the Regions. It also applies to bodies set up under secondary Community legislation, such as: the European Centre for the Development of Vocational Training, the European Foundation for the Improvement of Living and Working Conditions, the European Environment Agency, the European Training Foundation, the European Monitoring Centre for Drugs and Drug Addiction, the European Agency for the Evaluation of Medicinal Products, the Office for Harmonisation in the Internal Market, the European Agency for Safety and Health at Work, the Community Plant Variety Office, the Translation Centre for the Bodies of the Union, the European Monitoring Centre on Racism and Xenophobia, the European Agency for Reconstruction, the European Food Safety Authority, the European Maritime Safety Agency and the European Aviation Safety Agency. Finally, the European Data Protection Supervisor has to comply.

According to the second indent, activities of these institutions and bodies that fall completely within the second or the third pillar of the EU-Treaty are not covered by the regulation. In accordance with recital 16 of the regulation, the measures established by the data protection regulation should not apply to bodies established outside the Community framework, such as Europol or Eurojust. However, these bodies apply Convention 108 and have to respect fundamental rights (in accordance with Article 6 of the EU-Treaty; see recital 15 of the Regulation).

The third indent, finally, limits the application of the Regulation as far as manual processing is concerned. The meaning of this limitation can be found in Recital 15 of Directive 95/46/EC. A filing system is covered by the data protection rules, structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question. In general, in so far as a filing system permits an easy access to personal data, it falls within the scope of the Regulation. So, for instance, attendance lists of regular meetings organised by an institution that are stored in a paper file will usually be covered. It goes without saying that the limitation as regards paper filing systems becomes less important.

3.4.2. Data quality and lawful processing

Article 4 lays down the principles relating to data quality, and, *inter alia*, states that personal data must be:

- *Processed fairly and lawfully;*
- *Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes [...];*
- *Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; [...]*

This article constitutes one of the key elements of the data protection regulation, in general as well as in the context of this paper: disclosure of personal data to the public is to be regarded as an act of processing.

Article 4 requires that the disclosure of personal data:
- must have a legal basis (according to the first indent the processing must be lawful);
- must be in accordance with the purposes of the collection (the second indent explicitly states that the data should not be further processed in a way incompatible with the purposes of the collection).
  The finality is, in other words, decided at the time of collection of personal data. This second requirement naturally limits the type of public access that can be granted[40].

In order for the data processing to be lawful, it must fulfil the equally important conditions of Article 5. Accordingly, personal data may only be processed if:

- *necessary for the performance of a task carried out in the public interest on the basis of the EC Treaties or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed, or*
- *necessary for the compliance with a legal obligation to which the controller is*

[40] See, more in detail, chapter 4.

subject, or

- *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, or*
- *the data subject has already unambiguously given his or her consent, or*
- *necessary in order to protect the vital interests of the data subject.*

Article 5 plays an instrumental role when it comes to public disclosure of personal data as it defines whether such an act may be legitimate or not. The two first indents recognize the fact that a public administration or body is sometimes obliged to disclose personal data. In short, the data protection regulation opens up for an interpretation according to Regulation 1049/2001. If Regulation 1049/2001 requires disclosure, Article 5 of Regulation 45/2001 does not constitute an obstacle. The distinction between granting access on the grounds of the first indent - 5 (a) - or the second indent - 5 (b) - is very subtle, as the legal obligation to grant public access is general and giving effect to this obligation constitutes at the same time the performance of a task carried out in the public interest. The distinction has a legal effect in Article 18 (the data subject's right to object) - see 3.4.5.

The third and the fourth indent could also be relevant.
The third indent of Article 5 gives the institutions and bodies the right to disclose personal data to a third party who acts as an agent of the administration for the implementation of a contractual relationship. Indent four opens up the possibility for making personal data public, should the data subject have given it's unambiguous consent. This gives officials of the institutions and bodies a possibility to, in advance, ask explicitly for consent that a particular document may be made public.

Article 6 establishes the rules regarding change of purpose, which need to be respected, without prejudice to Articles 4, 5 and 10. Personal data

- *shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body;*
- *collected exclusively for ensuring the security or the control of the processing systems or operations shall not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences.*

In the first place, Article 6 is intended to give additional protection, but does not affect the safeguards the data subject is entitled to under the Articles 4, 5 and 10. In the second place, the first indent is worded restrictively. It only applies in case of a structural change of purpose which must be laid down in internal rules. It is not intended to prevent the disclosure of documents in individual cases, if Regulation 1049/2001 so requires. In the third place, the internal rules need to respect the treaties as well as secondary legislation. Internal rules that do not respect the transparency legislation may in that sense not be applicable.

3.4.3. Transfer of data

Three different articles (Articles 7, 8 and 9) regulate transfer of personal data, depending on the recipient. Article 7 deals with the transfer of personal data within or between Community institutions or bodies and falls outside of the framework of this paper.

Article 8 stipulates rules regarding transfer to recipients subject to the national law adopted for the implementation of the data protection directive. This includes public authorities in the Member States as well as the private sector and natural persons. Moreover, recipients residing or - in the case of legal persons - established in EFTA-countries are included. Article 8 allows for transfer under the condition that the recipient establishes:

- *that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or*
- *the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.*

The first indent of Article 8 is not relevant to the public access to documents, since Regulation 1049/2001, based on Article 255 EC, is designed to give access to documents to the public. This regulation is not meant to regulate the relations between the Community institutions and the public authorities of the Member States, not withstanding the fact that the latter could profit from the provisions of the regulation.

The second indent, however, is an illustration of the tension between the data protection regulation and the public access regulation, and moreover between the different objectives of the two regulations. A literal interpretation of the text would lead to a result which seriously impairs the effectiveness of the public access regulation. Such a result could not have been envisaged by the Community legislature. The second indent of Article 8 presupposes that the recipient of a document containing personal data establishes why he needs access to it. However, access to documents is given to enable citizens to participate more closely in the democratic process. It is essential to this objective that the citizen does not have to establish any specific interest in the disclosure of a document to him, as has been confirmed by the case law of the Court of first Instance[41].

The second indent should therefore be interpreted in the light of the objectives of the relevant provisions of both the data protection regulation and the public access regulation (the teleological method of interpretation). On the one hand, Article 2 of the public access regulation gives the citizen of the EU a legally enforceable right to access to documents, for the purposes that just have been mentioned. On the other hand, Article 8, second indent, merely envisages the protection of the data subject, in cases when the disclosure of the data is in itself allowed according to the provisions of Community law on data processing. In such cases the transfer of the data in itself would normally not prejudice his legitimate interests. In other words, if the transfer of personal data is allowed by the other provisions of Regulation 45/2001, Article 8, second indent, cannot restrict disclosure.

These considerations lead to the following interpretation: in cases where data are transferred to give effect to Article 2 of the public access regulation - and provided that the disclosure of the data is allowed according to the provisions of Community law on data processing - the necessity of having the data transferred is by definition established. Moreover, such a transfer cannot prejudice the legitimate interest of the data subject. In other words: a *necessary* transfer cannot prejudice *legitimate interests*, taken into account the conditions and safeguards provided by Regulation 1049/2001.

[41] See 2.4.1. hereinabove.

Article 9 regulates transfer of personal data to recipients that are not subject to the data protection directive, such as natural or legal persons in third countries, authorities of third countries or international organisations. According to Article 9, transfer is only allowed if an adequate level of protection of personal data is ensured in the country of the recipient or within the recipient international organisation. This prohibition also applies in cases where public documents contain personal data.

Regulation 1049/2001 does not affect the application of Article 9. In the first place, this regulation only confers a right to citizens of the European Union, and to natural or legal persons residing or having their registered office in a Member State. In the second place, despite this limitation the disclosure of a document under Regulation 1049/2001 *could* involve the transfer of personal data to a third country, for instance if the disclosure document is requested by a citizen of the Union, residing in a third country.

If disclosure involves the transfer of personal data to a country or to an international organisation that does *not* ensure an adequate level of protection of personal data, the exception of Article 4 (1) (b) of this Regulation would prevent disclosure, because the privacy an individual may be substantially harmed by disclosure.

3.4.4. Sensitive data

The regime covering sensitive data is established in Article 10(1):

> *The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited.*

The prohibition formulated in this important article is subject to a number of exceptions. The prohibition does not apply where the data subject has given his consent, if the processing relates to data that have been manifestly made public, or if it is necessary in order to protect the vital interests of the data subject. According to Article 10 (4) of Regulation 45/2001 - subject to additional safeguards, and for reasons of substantial public interest - additional exemptions may be laid down in community law. Regulation 1049/2001 contains such exemptions, since it defines for reasons of public interest and subject to its Article 4 (1) (b) that documents that can include personal data must be disclosed. In some cases, sensitive data may thus be made public, although the regime covering such information is much more restrictive (see, more in detail, Chapter 4).

Also, in case of processing of data relating to offences, criminal convictions or security measures additional requirements apply (Article 10 (5)). This provision could have relevance to data related to disciplinary procedures and measures of staff members of the institutions and bodies.

3.4.5. The rights of the data subjects

The data protection regulation also gives the data subjects a number of explicit enforceable rights. These provisions are a materialization of the general principle of fair processing as included in Article 4 of Regulation 45/2001. They include procedural safeguards for the data subject. On the one hand, the data subject has the right to be informed and to defend his legitimate interests on the basis of this information. On the other hand, the institution or the

body that has to decide on disclosure can act proactively and inform the data subject at an early stage about its intentions and ask the data subject, where appropriate, if he or she agrees to the disclosure.

Article 13 stipulates his right of access to his own personal data. As has been said in the introduction, this right of access in itself will not be elaborated in this paper. However, Article 13 also gives the data subject the right to, *inter alia*, be informed on the purposes of the processing, the categories of data concerned and the recipients to whom the data are disclosed.

Article 17 stipulates the right to obtain from the controller the notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking [...] unless this proves impossible or involves a disproportionate effort.

Article 18 on the data subject's right to object is of particular importance for the subject of this paper. The data subject shall have the right:

> *(a) to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her, except in the cases covered by Article 5(b) […] Where there is a justified objection, the processing in question may no longer involve those data.*

Article 18 makes a difference between processing covered by Article 5 (a) - necessary (...) in the public interest - and Article 5 (b) - necessary for the compliance with a legal obligation. Strictly speaking, the processing required by Regulation 1049/2001, constitutes a legal obligation as meant in Article 5 (b). As a consequence, the data subject would not have a right to object. However, such a consequence would be unsatisfactory since the legal obligation to disclose a document containing personal data as foreseen by Regulation 1049/2001 is not unconditional. Article 4 (1) (b) provides for an exception that explicitly refers to the community legislation regarding personal data and requires that the effect of the disclosure on the data subject is taken into account. Under those circumstances, denying a right to object to a data subject - an essential element of data protection - would not make sense since the opinion of the data subject is of importance to the decision on disclosure.

Article 18 should be interpreted in a way that it only denies the right to object to a data subject if the legal obligation to disclose or otherwise process personal data is of an unconditional nature. In such a case, a right to object would be meaningless. Such an unconditional obligation can, for example, be found in Article 25 (3) of the Staff Regulations (see 2.4.2).

This leads to the conclusion that under Article 18 the data subject has a right to object, if disclosure is requested under Regulation 1049/2001.

However, one should keep in mind that an obligation to inform all the data subjects in advance -so as to give effect to their right to object - would be disproportionate and would prejudice the effectiveness of Regulation 1049/2001. Consequently, the following approach would do justice to the text of Article 18 and to the principle of proportionality: the community institution or body involved should only ask the opinion of a data subject before deciding on disclosure, when it is likely that the privacy of the data subject could be

substantially affected by the disclosure of a document[42]. The opinion of the data subject on the effects of the disclosure to his privacy will - in those cases - be one of the elements to be taken into account by the decision making authority.

3.4.6. Exemptions and restrictions

Article 20 of Regulation 45/2001 gives the Community institutions and bodies the possibility to restrict the application of *e.g.* Article 4 (1) of the Regulation. If such a restriction is imposed the data subject shall be informed of the principle reasons and he has a right to have recourse to the EDPS (Article 20 (3)).

The exemptions and restrictions of Article 20 are exemptions to the balanced system of Regulation 45/2001. They deprive the data subject of essential elements of the protection he is entitled to according to the regulation. Under Community law, such exemptions should be interpreted restrictively. It has to be emphasised that Article 20 is meant for exceptional cases where the protection of the data subject, based on Article 4 of the regulation, would harm other fundamental public interests. Regulation 45/2001 provides for an explicit reasoning in every individual case when the restriction of Article 20 is applied. This reasoning is subject to examination by the EDPS (and, in a final stage, by the Court of Justice).

It is for these reasons that Article 20 is of no importance in the context of this paper. The system provided for in Regulation 1049/2001 and 45/2001 allows a balancing (or a proportionality test) between the public access and the protection of the data subject, and thus guarantees the public interest of public access. Under such circumstances there is no need for an additional exemption under Article 20.

3.5. The Charter of Fundamental Rights and the Constitution

The Constitution explicitly establishes that 'Everyone has the right to the protection of personal data concerning him or her'. Under the Constitution this right, which has already been recognised in the existing Charter of Fundamental Rights of the Union, gets a binding character and can be enforced before the courts.

In fact, the Constitution mentions the right to data protection twice:

- In Title VI on the democratic life of the European Union, next to the provisions on transparency and public access to documents and the role of the Ombudsman (Article I-51). This positioning clearly indicates that the protection of personal data is regarded as an essential ingredient of good and responsible governance.
- In the Charter of Fundamental Rights which constitutes part II of the Constitution[43] Article II-68 sums up the main elements of the right to data protection: substantive principles, individual rights and independent supervision. In the Charter, a separate reference is made to the respect for private and family life; established in Article II-67. This clearly illustrates the fact that the both notions feature different, albeit interlinked, characteristics.

[42] According to the criteria of 4.3.3 and 4.3.4.
[43] See Par. 2.6, on the legal status of Part II of the Constitution.

Furthermore, Article I-9 (3) repeats the wording of Article 6 (2) of the EU Treaty regarding the respect of fundamental rights, as guaranteed by the European Convention on Human Rights, and introduces the respect of fundamental rights as a general principle of EU law.

The second subparagraph of Article I-51 lays down that the protection of personal data shall be governed by a European law, which regulates the processing both on the level of the Community institutions and bodies and on the level of the Member States.

4. Simultaneous application of the regulations

4.1. Introduction

This chapter is on the simultaneous application of two obligations of the Community institutions and bodies.

On the one hand: the Community institutions and bodies have to give the European citizens the widest possible access to documents (see Chapter 2 for more detail), so as to ensure the effectiveness of the (fundamental) right to access to public documents as has been recognised in the EC-Treaty and implemented in Regulation 1049/2001 and other legal instruments in cases where this regulation does not apply. Access to documents must be seen as an important instrument to promote participation in the decision-making process by public bodies and to enhance the accountability of the administration vis-à-vis the citizens.

On the other hand: the institutions and bodies must offer protection to individuals with regard to the processing of personal data (see more in detail Chapter 3), so a to ensure the effectiveness of the (fundamental) right to data protection that has been conferred to individuals, according to Regulation 45/2001, or according to other legal instruments where this regulation does not apply. This right fully extends to personal data contained in an official document or held by a public administration or body.

The Community legislature has recognised that both obligations can be applicable at the same time and collide. Article 4 (1) (b) of Regulation 1049/2001 states that 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. Regulation 45/2001 allows for the disclosure of personal data, if this is necessary for the performance of a task carried out in the public interest and/or for the compliance with a legal obligation (see Article 5 of Regulation 45/2001), such as rendering public access to a document.

The Community legislature recognises the possibility of collision, but does not give clear guidance on how to act, if a collision occurs. In addition, it should be noted that the two rights are of equal importance and grouped together in the Constitution, notably under the title 'the democratic life of the Union'.

This chapter aims to give the necessary guidance to the responsible authorities within the Community institutions and bodies on how to act if both rights (or, seen from the perspective of the EU-institutions and bodies: obligations) apply at the same time. Chapter 5 will illustrate some experiences with this situation.

This guidance might be helpful:

* before personal data have been collected (the proactive approach):
    - to establish procedures,
    - to develop technological systems, or
    - to adopt internal rules on the access to certain documents containing personal data.

* in cases where data have already been collected (the reactive approach), the decision to make:
    - when an individual asks for access to a document that contains personal data;
    - whether a document containing personal data will be published;
    - when public access has been given to a document and the data subject lodges a complaint.

4.2. Guiding principles

4.2.1. The perspective: Article 4 (1) (b) of the public access regulation

As has been said, the texts of the two regulations do not give guidance on how to act when both regulations are applicable at the same time. One could approach the matter from the perspective of the public access regulation, notably its Article 4 (1) (b), or from the perspective of the data protection regulation. This paper chooses the first perspective. It will determine under what conditions Article 4 (1) (b) should apply.

Article 4 (1) (b) of Regulation 1049/2001 is appropriate as a starting point for a balancing of the two legitimate interests. It refers to the data protection regulation, and, by giving this reference, it explicitly deals with the relationship between the two regulations. Moreover, the issue will most likely arise in cases when a decision must be taken on the access to certain documents.

4.2.2. The principle of the right to information and the principle of proportionality

The paper takes into account the case law of the Court of Justice, in particular its Judgment in the Council v Hautala case[44]. The Court of Justice has recognised that when personal data are at stake the rules on public access must be interpreted in the light of:

- the principle of the right to information. The aim pursued by the public access provisions 'is to provide the public with the widest possible access to documents held by the Council, so that any exception to that right of access must be interpreted and applied strictly'. Moreover, the principle of access to documents should not be applied only to documents as such, but also to the information contained in them. Lastly, the principle of the right to information implies that it is the party who requests, not the institution or body holding the document, that decides whether it is of interest or relevance for him or her. It is in that respect irrelevant that an institution finds the document of little use for the applicant when it deals with the request for public access.

- the principle of proportionality. The exceptions to the right of public access to documents need to be subject to a proportionality test. Derogations shall remain within the limits of what is appropriate and necessary for achieving the aim in view[45]. Moreover, the proportionality test obliges an institution to examine whether partial access should be granted to the information not covered by an exception.

[44] C-353/99 P, quoted in Footnote 17. The analysis of this case is based in particular on the Paragraphs 25-31 of the Judgment.
[45] Paragraph 28 of the Judgment.

Furthermore, reference is made to two authoritative policy papers in this area. The Article 29 Working Party does not refer to the principle of proportionality, but construes a case-by-case approach based on a balancing of the two fundamental rights, by stating as follows[46]:

"Given that the obligation of administrations to grant public access to documents is limited by their obligation to protect personal data [...] 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 in each particular situation, and therefore whether the request for access should be satisfied or rejected."

Support for this approach can be found in the report of the Commission on the implementation of the public access regulation. Although characterizing the exceptions of Article 4 (1) of the regulation as compulsory and absolute, the Commission states[47]:

"The decision on whether to grant access to documents containing personal data must be based on the balancing of the interests at stake, on the one hand the need to inform the public and, on the other, the protection of the persons concerned. This balancing exercise must be carried out in each case, with due regards to all the circumstances involved."

'Balancing' and 'proportionality' are not identical, but can lead to a similar result. Both criteria imply that Article 4 (1) (b) can not be applied mechanically. An analysis of the different elements should take place on a case-by-case basis, where all relevant elements are taken into account. The purpose of a concrete and individual examination is to see the extent to which an exception is applicable. The Court has established that any exception to the general rule (concrete and individual examination of each requested document) may only take place if it is obvious that access must be refused or, on the contrary, granted. Such could be the case if, for example, a certain document is manifestly covered in its entirety by an exception or, conversely, manifestly accessible in its entirety, or, had already been the subject of a concrete, individual assessment by the Commission in similar circumstances.

4.2.3. Partial access and the notion of 'unreasonable amount of administrative work'

As has been stated, public access to documents is an approach to be adopted in principle; the possibility to refuse access is the exception. That, in combination with the principle of the right to information must be interpreted in the light of Article 1 of the public access regulation which grants the public the widest possible access. This leads to the conclusion that in those cases where the proportionality test, based on a concrete and individual examination, has shown that full access would undermine the privacy of an individual, the possibility to grant partial access must be considered. In the Council vs. Hautala-Judgement, the Court stated that the exercise of removing certain passages or data in a document should be conducted unless it would result in an unreasonable amount of administrative work.

It has to be mentioned that such a solution is not always appropriate, since in some cases the reference to personal data is the heart of the document. While a certain complaint with the European Ombudsman could be of almost equal value in an anonymised version (because of

[46] WP 29 Opinion 5/2001 p. 5, see Footnote 3.
[47] Report from the Commission on the implementation of the principles in EC Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents, p. 19, see Footnote 14.

the policy shaping value of the decision), this would not at all be the case in a request for public access to a shortlist of candidates for a particular high-level post at the Commission

In the Konsumenteninformation vs. Commission case[48], the Court of First Instance elaborated upon the notion of 'unreasonable amount of administrative work' and specified that the possibility to refrain from doing a concrete and individual examination of a document only exists in exceptional cases. In the Judgement (the case concerned a public access request for a 47.000 page file), the Court gave no support to the decision of the Commission to classify the pages in categories and then state that each category was subject to an exception. The Court also referred to Article 6 (3) of the public access regulation and the possibility for an institution to confer with the applicant informally, with a view to finding a fair solution. The Court also recalled the possibility for an institution to prolong the handling time of a request, in accordance with Article 7 (3) of the same regulation.

4.2.4. Interpretation in the light of Article 8 ECHR

As we have seen in Chapter 3, Community legislation on data protection must be interpreted in the light of fundamental rights, in so far as it deals with processing of personal data liable to infringe fundamental freedoms recognised in the European Convention on Human Rights, in particular the right to privacy.

The exception to public access in Article 4 (1) (b) of the public access regulation deals by definition only with personal data liable to infringe the right to privacy. Any decision taken under Article 4 (1) (b) must respect Article 8 ECHR: the disclosure of a document may not have as an effect that Article 8 ECHR will be infringed.

In practice, the authorisation of restrictions to the right to privacy, under Article 8(2) ECHR will - within the framework of Article 4 (1) (b) of Regulation 1049/2001 - not require an additional assessment. Article 4 (1) (b) itself will provide the required legal basis: which has as a result that the restriction to the right to privacy will be 'in accordance with the law'. The concept of 'necessary in a democratic society' is - according to the case law of the European Court for Human Rights - comparable to the concept of proportionality[49]. It involves a balancing of all the relevant interests and factual circumstances[50].

In the Peck-case[51], the Court of Human Rights makes an interpretation of an alleged violation of Article 8 of the Convention on Human Rights. The Court analyses two questions: whether the interference to privacy was in accordance with the law and pursued a legitimate aim; and whether this interference was justified. On the latter point, the Court makes the general remark that in cases concerning the disclosure of personal data, the competent national authorities shall dispose a margin of appreciation in order to strike a fair balance between the relevant conflicting public and private interests[52]. In the case of a tension between the public

[48] Case T-2/03, Judgment of 13 April 2005, text of the judgment available on: http://europa.eu.int/cj/en/content/juris/index.htm

[49] Although it concerns *strictly spoken* the proportionality of the exception to the protection of privacy (and not, like the Council vs. Hautala-Judgment, the proportionality of the exception to public access).

[50] See, P. van Dijk and G.J.H. van Hoof, Theory and Practice of the European Convention on Human Rights, Third Edition, The Hague 1998, p. 537.

[51] Judgment of 28 January 2003, Reports 2003-I.

[52] P. 18-19. The same margin of appreciation applies of course to Community institutions and bodies.

access and the data protection regulation, the justification has to be found within these boundaries.

4.3. The analysis of Article 4 (1) (b) of the public access regulation

4.3.1. Do both regulations apply?

One should keep in mind that Regulation 1049/2001 on the one hand and Regulation 45/2001 on the other hand have different scopes, as well as different aims.

As to the different scopes: Regulation 1049/2001 is limited to documents drawn up or received by and in the possession of the European Parliament, the Council and the Commission. But, as was shown in chapter 2, most other institutions and bodies have adopted similar rules on a voluntary basis.

Regulation 45/2001 is limited to the processing of personal data by the Community institutions and bodies insofar as it is carried out in the exercise of activities all or part of which fall within the scope of Community law. The regulation applies 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 (see on the limitations as regards paper files: 3.4.1).

A restrictive interpretation of Regulation 45/2001 gives that it, in this aspect, only covers first pillar activities. It may thus be possible to find cases that would fall outside the scope of the regulation. However, as all Member States of the EU have ratified the European Convention on Human Rights as well as Convention 108, those cases would still be guided by these two conventions, as interpreted by the case law of the European Court of Human Rights. Furthermore, support can be found in Article 8 of the Charter of Fundamental Rights of the European Union.

Summarized: The principles stemming from Regulation 1049/2001 and Regulation 45/2001 have a wide field of application. The limitations of the scopes of the regulations themselves do not have as an effect to delimit the areas in which the rules on public access and on data protection both apply.

As to the different aims: the public access regulation strives towards the widest possible openness when it comes to the processes through which public bodies make decisions as well as the information on which those decisions are based. By analogy, it strives towards the easiest possible exercise of these rights, as well as towards the promotion of good administrative practices. On the other hand, the data protection regulation strives to protect the individual's fundamental rights and freedoms, notably their right to privacy when personal data are processed.

The two different aims seldom collide. Privacy (and integrity) of the individual is but one exception to the automatic granting of public access to documents, and it should be seen as just that, in the context of the exhaustive list of exceptions that is laid down in (Article 4 of) the public access regulation.

Most often, a document sought for can be handed out without undermining a person's right to privacy - the mere fact that a document contains personal data does not mean that a person's

privacy is involved. In many cases, official documents contain personal data. However, only in a certain number of these cases - depending on the circumstances - is the privacy of a person involved. Only in these cases may a collision with the public access regulation occur. It is the task of the responsible authorities to ensure that the protection of the privacy of the data subject does not have disproportionate effects on the interest of transparency.

Summarized: both regulations do not collide by definition. In many cases public access can be given without any prejudice to the legitimate interests of the data subject.
But, as will be shown in the next paragraph, collision does not always lead to a difficult appraisal. To the contrary:

- in quite a few cases rendering partial access to a document - by deleting references to persons - would be a logical and effective solution to reconcile the two fundamental rights;
- quite often a solution can be offered beforehand, by informing the data subject about the use that will be made of the personal data he of she renders to a Community institution or body (the proactive approach).

4.3.2. The actual analysis: Introduction

Once it has been determined that a document falls within the scope of Regulation 1049/2001 (or a similar legal instrument) and no other provision prohibits access, the decisive question is: does the exception of Article 4 (1) (b) apply?

To this extent, three conditions must be fulfilled:

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.

The analysis results in a checklist, that is inserted in Chapter 6.

4.3.3. Condition 1: Is the privacy of the data subject at stake?

Many documents contain some personal data. But, since under Article 4 (1) (b) of Regulation 1049/2001 access to documents shall only be denied if the protection of privacy (and the integrity) of the individual is undermined, it has to be determined whether the interest of the data subject that is affected falls within the scope of the protection given by Article 8 ECHR.

As has been demonstrated in Par. 3.2.2, Article 8 ECHR goes beyond the protection of private life and may not be interpreted restrictively, but is not endless. The following guidance can be given:

- There must be a qualified interest of a person involved, which means that the document must contain details about a person that are normally regarded as "personal" or "private".
- The fact that a document contains personal data of a general character like the name of a person should (in general) not hinder disclosure.
- The notion of private life does not exclude activities of a professional or business nature, but the interests involved may have a different character.
- Disclosure of data would normally fall within the scope of protection, if:
    - sensitive data as mentioned in Article 10 of Regulation 45/2001 are involved, such as for instance data concerning health;

- the honour and reputation of a person is involved;
- a person could be placed in a false light;
- embarrassing facts would be disclosed;
- information given or received by the individual confidentially would be disclosed.

N.B. 1: This indicative list serves just as a guidance, and is subject to review by the competent judicial authorities.
N.B. 2: This list does not determine whether information may be disclosed; it just points out whether the privacy of the data subject is at stake.

Acting in a public capacity - an exception to the right to privacy?
Employees in a public administration must be aware that for several reasons, their personal data may be of public interest to a degree different from the situation where he or she would be working in the private sector. Two such interests are accountability and transparency. For those reasons, certain personal data (such as the name and function of an official) can, in general, be disclosed without consent, provided that it is appropriate and motivated by the activities of the institution.

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 institutions or bodies. It therefore follows that 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 employees on a higher level, when they represent Community institutions or bodies. Needless to say, the personal data would still be subject to the rules of the data protection regulation.

Furthermore, if a document refers to, for instance, what a Commissioner has stated in the exercise of his or her duties it would make no sense to examine whether or not his or her privacy would be at stake.

The following example, on Members of the European Parliament, illustrates the matter.

> The minutes of a meeting at the European Parliament can be made public for several reasons. Being a Member of the Parliament is a public post and the information on which committee he or she is assigned to is public. It can be expected that a member of a committee attends a meeting, and when expressing his or her view the member exercises the role of a parliamentarian. As the possibility of public access has also been clarified in the rules of procedure of the Parliament, the case becomes a rather obvious example of where privacy could not be claimed.

Summarized: the privacy notion extends in general also to the work place. Also public officials have a right to privacy at work. However, the privacy notion does not always extend to people acting in a public capacity.

4.3.4. Condition 2: Is the data subject substantially affected?

Public access must substantially affect the privacy of a data subject.

This condition is closely linked to condition 1. However, there is an essential difference:
- Condition 1 requires an examination whether the information contained in a document falls within the scope of Article 8 ECHR.
- Under condition 2 it has to be examined whether, in the specific case, disclosure would undermine or, in other words, substantially affect the privacy of the data subject.

In quite a few cases, public access to a document does not affect the privacy of the persons that are mentioned in a document, or has only superficial consequence on privacy. One could think of the disclosure of data in a document which have already been made public at an earlier occasion. Other examples might involve the mentioning in a Community document of a report written by a certain expert, in which he reveals sensitive data, or the mentioning of a reference to an amendment made by a Member of the European Parliament in which he expresses his political views.

Summarized: it must be examined whether the privacy of a data subject is substantially affected, i.e. if the consequences for his or her privacy are not merely theoretical. This examination - as in the previous paragraph - requires a careful evaluation of the relevant details and the context of the case as they should be observed from an objective perspective.

NB: When the community institution or body considers it to be likely that the privacy of the data subject could be substantially affected by the disclosure of a document, it asks the opinion of the data subject before deciding on disclosure (see 3.4.5).

4.3.5. Condition 3: Public access can only be given if this is allowed by the data protection legislation.

It is at this point that the principle of the right to information and the principle of proportionality as formulated by the Court of Justice in the Council vs. Hautala case play a key role.

<u>The principle of the right to information</u>
As has been stated before, any exception to the right to information must be interpreted and applied strictly. The exception of Article 4 (1) (b) of Regulation 1049/2001 may be applied only insofar as Regulation 45/2001 explicitly prohibits the disclosure of data.

The analysis in Paragraph 3.4 of this paper showed the most relevant conditions in Regulation 45/2001 concerning the disclosure of personal data. In connection with the principle of the right to information, these conditions should be understood as follows:
1. Disclosure of personal data must be compatible with the purposes of collection, as has been decided at the time of the collection of personal data (Article 4 of Regulation 45/2001). If, at the time of the collection of personal data, the purpose of collection excluded disclosure to third parties - explicitly or implicitly - public access would infringe Article 4. This requires an examination of the precise consequences of the purpose, as mentioned to the data subject at the time of collection. How the data subject could reasonably understand this purpose should be taken into consideration.

2. In many cases a proactive approach can help alleviate potential tensions beforehand. It can be helpful to inform the data subjects beforehand, at the time the data are collected, that the personal data might be made public.
3. However, no matter what information has been given to the data subject: all the conditions mentioned in Article 4, must be fulfilled. In particular, the processing must be fair and lawful and the data must be adequate, relevant and not excessive, in relation to the purposes for which they are collected.
4. Moreover, the purpose can not be changed afterwards, by giving additional information to the data subject.
5. Article 10 lays down 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.

Conclusion: No public access can be given if this would infringe Article 4 or Article 10 of Regulation 45/2001.

Article 5 of Regulation 45/2001 allows disclosure if necessary for the performance of a task carried out in the public interest or necessary for the compliance with a legal obligation. On the one hand, Article 5 facilitates public access, if this is necessary to comply with the public access regulation or (with the same result), to perform the task as formulated in that regulation. On the other hand, Article 5 limits public access, since it does not allow the 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.

<u>The principle of proportionality</u>
The proportionality test consists of 2 elements:

1. As the Court stated in Council vs. Hautala case, derogations to public access should remain within the limits of what is appropriate and necessary for achieving the aim in view.

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.

Ad 1: It has to be analysed what relevance the disclosure has to the protection of personal data: to what extent are the rights of the data subject as safeguarded by Regulation 45/2001 affected. In other words: what kind of harm does the disclosure do to the data subject?

The analysis will have to take into account:

- the compulsory or voluntary basis of the original data collection about the data subject;
- the kind of personal data processed;
- the situation of the data subject and the potential consequences of public disclosure for him or her;
- disclosure causes less harm to the data subject if the document is handed over upon request than if it would be published in the Official Journal of the EU as the number of recipients a document would be submitted to would be less.

In any case, the result of disclosure may not be that a private person will be deprived of, or unduly restricted in the exercise of, his or her (fundamental) right to data protection.

Ad 2: If unlimited disclosure of a document would deprive of or unduly restrict the data subject in the exercise of his or her (fundamental) right, less restrictive measures have to be taken into consideration. One should consider giving partial access to a document, for instance by erasing, blocking or deleting personal data or references to personal data before handing over the document to a third party.

Additionally, the data subject could be informed of the intention to give access and be allowed to give his or her opinion (see, Par. 4.3.4).

5. Experiences within the EU institutions and bodies

5.1. Introduction

As both the data protection and the public access regulation have been in force since 2001, officials of the institutions and bodies have already dealt with a wide range of requests for documents containing personal data. The following examples, partly drawn from this experience and somewhat revised where appropriate, aim to give an indication as to what result the analysis of Article 4 (1) (b) of the public access regulation might lead to. They are not designed to decide individual cases where additional facts may influence the outcome.

The examples are divided into two sections, depending on whether the example is more related to a proactive approach or more related to a reactive approach. Both categories contain situations in which it was deemed necessary to only grant partial access, as full disclosure would have undermined the protection of the privacy of the individual. The comments to the examples follow the main points of the check-list of Chapter 6[53].

Examples can be found in different categories of personal data being made public, such as:

- in relation to employment procedures;
- due to a request for information on employees;
- due to a request for information on attendance at meetings or presence in buildings;
- due to being part of a dossier in a complaint procedure.

5.2. Examples of a proactive approach

Every institution and body has the possibility to adopt complementary documents in order to clarify the use of personal data, the rules on public access, etc. Accordingly, an institution may use, for example, its rules of procedure, its employment procedures or its staff regulations in order to clarify that a specific document may be disclosed, in accordance with the objectives of the transparency regulation.

This type of supporting documents enhances compliance with the data protection regulation that allows for disclosure of personal data, if expressly permitted by the internal rules of the institution or body and in accordance with the safeguards of the data protection regulation. The use of additional documentation in order to clarify and promote compliance with both regulations, and thereby promote both rights, receives full support from the EDPS. In this context, it is worth underlining that proactive documents naturally must respect the principles of legitimate processing, particularly those laid down in Article 5 of the data protection regulation.

Example 1: The European Ombudsman complaint form

One of the most explicit examples of a proactive measure may be found in the complaint form of the European Ombudsman. The form states:

"Dealing publicly" with a complaint means that any member of the public may have access to the complaint and its annexes. If the Ombudsman opens an inquiry, the opinion of the

[53] As the steps [A] to [C] are given for granted in the examples, and for reasons of limiting the size of the paper, the analysis does not comment upon those steps.

institution or body concerned on the complaint, any observations on the opinion made by the complainant [...] are public documents to which any member of the public may have access on request. [...] A complainant has the right to request that his or her complaint be dealt with confidentially. If confidentiality is requested, there is no public access to the complaint or to the other documents mentioned above. However, even a confidential complaint must be sent to the Union institution or body concerned, if the Ombudsman begins an inquiry. The Ombudsman's decisions on confidential complaints are published in his Annual Report and on his Website, after the removal of any information which could lead to the identification of the complainant."

Complainants are asked for consent if specific categories of citizens (such as journalists) ask for access to their files.

Comment:
Is the privacy of the data subject at stake?
It is clear that a complaint and any subsequent documents can contain personal data regarding the complainant as well as third persons. Arguably, the information given by a complainant or received from others relates in many cases closely to the privacy of those persons.

Is the data subject substantially affected by disclosure?
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 whether the complaint should be dealt with publicly or not. 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. Moreover, the complainant is informed that, independently of which box he or she ticks, limited public disclosure will be a fact as the circumstances of the complaint will be made public.

Public disclosure of the decision on a complaint where the complainant has opted for confidentiality would breach Article 4 of the data protection regulation, 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. Disclosure can not be seen as a proportionate measure and it is therefore legitimate to allow partial disclosure, instead of full access.

Conclusion:
It is the policy of the Ombudsman to deal with complaints in general in public and to publish the decisions on the website by mentioning the first letter of the name of the complainant. Although 'unambiguous consent' is an important factor when it comes to disclosure, it is not decisive. In any case, the obtained consent can only be used for the purposes it was collected - the consent of the data subject for public treatment allows for public access, but does not extend to other types of processing that he or she was not informed of at the moment of giving consent.

When it comes to access to the complaint file, which is a slightly different question, it is important to bear in mind that some of the documents relating to the investigations of the

Ombudsman are confidential and shall not be made public[54]. The fact that the Ombudsman asks the complainant for consent for disclosure of the file respects the rights of the data subject. Naturally, a request from the data subject to his or her file would be governed by the rights of the data subject and the data protection regulation, rather than the public access regulation.

Finally, one must bear in mind that even though a complainant may agree fully with disclosure, third parties have no say in whether the complaint should be made public. The practical solution to guarantee the rights of third party data subjects must therefore be to test the proportionality of revealing facts relating to them in accordance with the 4 (1) (b) exception.

Example 2: Should the results of a competition be published?

When applying for a competition organised by EPSO, the applicant is informed that the results of the competition will be published in the Official Journal as well as on the website of EPSO. The names will thus, in most cases, be published before the people on the reserve list are actually recruited. To deal with specific individual problems that can arise from public disclosure, applicants are informed that they can put forward reasons why their names should be removed from the list during the selection procedure. The reserve list may, as a consequence, not show all the names of the candidates who passed the competition.

Comment:

Is the privacy of the data subject at stake and is the data subject substantially affected?

In this case, EPSO has decided to publish the names of the people who have not argued that their privacy would be seriously affected by disclosure. In most cases, the mere disclosing of the name of a person and the fact that he or she has passed a competition does not mean that his or her privacy is involved. However, in the case of recruitment procedures, one must keep in mind that certain employees could be subject to disadvantages from their current employers, would it be known that they succeeded in a competition. The privacy of a data subject can thus be involved, as the notion privacy extends to the workplace. The data subject may be substantially affected, for example should he or she have difficulties in receiving further promotions.

Is disclosure allowed according to data protection legislation?

In view of the fact that EPSO informs the candidates of public disclosure during the selection procedure when the data are collected, disclosing the names of those who have not opted out, is in compliance with Article 4 of the data protection regulation. On the other hand, to disclose the name of a candidate who has asked for confidentiality on legitimate grounds would be incompatible with Article 4. Moreover, the consent (for disclosure of the name) does naturally not extend to other documents that EPSO has received, such as certificates proving previous working experience, or the answers in the exams themselves.

The public interest in the result of a competition is reinforced by reasons of accountability. It is therefore legitimate and appropriate to reveal the names of those who succeeded in the ways indicated. This does not mean that all personal data which were collected during the application procedure should be subject to public disclosure; public access must remain within the limits laid down in Article 5 - in other words, the disclosure must be necessary for

[54] This is reflected in the Decision of the European Ombudsman adopting implementing provisions (Article 14).

the performance of a public task or to comply with a legal obligation as laid down in the public access regulation.

Conclusion:
This example provides for general publicity of some personal data to ensure accountability. The relevant information is given at an early stage and applicants have an opportunity to opt-out for legitimate reasons. Other personal data of applicants remain fully protected.

Example 3: Information given to the candidates for a public post regarding their C.V., which will be put on-line should they be offered and accept the post

Previously, if someone asked for access to the C.V.'s of persons on certain posts of a public character, such as general directors and spokespersons, certain personal data (such as the private address of the person concerned) were deleted, and only partial access was granted. Today, candidates are informed that their C.V. will be published on the Internet, should they accept the post and they are asked not to include information on their marital status, family status and address in their C.V. A specific C.V. form will be developed for this purpose.

Comment:
Is the privacy of the data subject at stake and is the data subject substantially affected?
Recruitment procedures comprise a selection phase during which confidentiality in many cases is important for the data subjects. If their data would be disclosed, the candidate may suffer negative consequences with their current employer and their privacy can thus be substantially affected. Once a candidate is recruited to a public body, public interest will be high for reasons of accountability, especially so in the case of more public posts. A proactive approach - providing for CV's with less personal data - can help to combine the interests at stake.

Is disclosure allowed according to data protection legislation?
In the old system, the C.V. contained personal data which relate closely to the privacy of the individual, such as marital status. Disclosure of such information would run contrary to the purposes of collection and it would be incompatible with Article 4, and its processing was not necessary for a good performance of the public task as envisaged in Article 5.

In the new system, the candidates are requested not to enter marital status, family status or their private address in the C.V. Civil servants holding a more public post shall be aware that there is a legitimate interest in them, and in that sense a higher threshold for privacy to be invoked. The new, proactive, system allows for direct publication of the C.V. once the candidate has accepted the post. As the candidates have been informed of this type of public disclosure, it does not infringe Article 4. That, however, does not mean that all personal data of the application file, such as all elements of the cover letter, can be disclosed - the file of the data subject is still safeguarded by the data protection regulation.

Conclusion:
This example clearly distinguishes between the needs of a selection and the appointment phase, and provides for general publication of a CV with only relevant data. Adequate information is given to enable candidates to take an informed decision. Other personal data remain fully protected.

Example 4: Should the name of a petitioner be put on the website of the European Parliament?

The Committee on Petitions of the European Parliament provides general information as well as a petition form on their website. The form 'Procedure for submitting a petition to the European Parliament' states in point 5: 'If the subject of your petition falls within the remit of the European Union it will normally be declared admissible and its contents considered'. Point 7 continues: 'Petitions are entered in the general register and are announced at plenary sittings of the European Parliament. These announcements appear in the minutes of the sitting'. The petition form asks the following question: 'If the Committee on Petitions declares your petition admissible, do you agree to its being considered in public?'. The entry page of the Citizens' portal which gives access to the information above informs that there are three categories of petitions: 'a matter of general concern', 'an individual grievance' or 'an appeal to the European Parliament to take a stance on a matter of public interest'.

Comment:

Is the privacy of the data subject at stake and is the data subject substantially affected?

Petitions can deal with all kinds of subjects, of which some are privacy related, while others are not. The petitioner is informed at the time of filing the petition that independently of which category the petition will belong to, his or her name and petition number will be mentioned during a plenary session. The petitioner will thus (irrespective of whether he or she chooses 'confidential treatment') be subject to limited public disclosure. That is an effect of the petition procedure, as foreseen in the Treaty, having a public nature. To that extent in any case, interested parties are made aware of the consequence that by submitting a petition, the petitioner is actively involved in the public debate. The name and petition number of the petition are announced during a plenary meeting. They are also reflected in the minutes of the meeting. Sometimes, such a list of petitions comprises some 200 entries - which naturally encompass all three categories mentioned above.

The privacy aspects of many petitions which concern 'a matter of general concern' or 'an appeal to the European Parliament to take a stance on a matter of public interest' will be relatively low. On the other hand, 'an individual grievance' is naturally more likely to have important privacy aspects.

Is disclosure allowed according to data protection legislation?

Consent, as defined in Article 2 (h) of the data protection regulation, is obtained for disclosure of the name and the petition number in a public meeting and such public disclosure does not infringe Article 4. However, it is not clear as to whether the reference to a general register and minutes of a meeting would always lead to 'unambiguous consent' in the sense of Article 5 (d) for publication of the name of the petitioner on the website of the European Parliament. In any case, such consent has not been given to disclose other personal data.

The privacy related problems are addressed by the possibility that the petitioner can choose whether his or her petition should be dealt with publicly or confidentially. When it comes to dealing with the petition in the Committee, as well as access to other documents in the petition file, it is imperative that complaints (should the petitioner not give any indication when filing it) are treated confidentially, as they may contain privacy related and/or confidential information. Any request for access to related documents needs to be subject to a concrete and individual examination where the proportionality of disclosure is analysed. To

deal publicly with a complaint, if the petitioner has not given informed and explicit consent for it, would infringe both Articles 4 and 5 of the data protection regulation.

Naturally, if the data subject asks for access to his or her file with the Committee on Petitions, access should be granted on the basis of the data protection regulation rather than the public access regulation.

Conclusion:
This example clearly distinguishes between different degrees of publicity in different stages of the procedure and provides for information allowing petitioners to make up their mind at an early stage. That information could still be improved by a clear reference to publication on the website, since this may not be fully evident to all concerned, possibly also allowing an opt-out for legitimate reasons warranting a lower degree of publicity at that stage. Publicity as a general principle is however clearly inherent in the functioning of the European Parliament.

5.3. Reactive approach

An institution or a body may have to assess the legitimacy and proportionality of disclosing personal data in different cases, such as:
- an individual asks for access to a document that contains personal data;
- a decision has to be made as to whether a document containing personal will be published;
- public access has been given and the data subject lodges a complaint.

Example 5: Can a newspaper get a list of staff of its nationality within the institutions?

A newspaper may want to have information relating to the staff of the institutions, such as statistics on employees of its nationality or a specified list which mentions the name, the grade, the institution and the place of work (city). A legitimate interest, although none has to be proven, is the control function that media play in how the institutions make use of the tax payer's based budget.

Comment:
Is the privacy of the data subject at stake and is the data subject substantially affected?
The level of privacy involved depends naturally on what type of request it is and on what information is subsequently made public. If, for instance, only statistics are made public, there would be no privacy involved at all, apart from exceptional cases where the level of detail makes it possible to identify specific individuals and the information relates to his or her private life.

In the case were the name and the grade of the official are made public, the privacy implications will naturally increase. Such information might, in combination with other official documents such as the salary scale, lead to a closer connection with the private life of the person. On the other hand, as was stated in section 4.3.3, employees of a public body must be aware that there is a stronger public interest in them as public officials, than if they would work in the private sector. The higher the grade, the more relevant this will be.

In general, to establish and disclose a list which contains the name, the place of work and the nationality of a group of officials is legitimate, as long as the people are not subsequently deprived of their rights as data subjects. Given the context, it is difficult to see that disclosure of the name and place of work of officials in a higher grade (together with similar staff of the same nationality) would affect the privacy of the individual. Exclusion from the list (and a

right to be anonymous) can here only be justified in exceptional cases; such as if the official has a confidential address, or has previously been exposed to threats. Only then can the data subject be judged to be substantially affected by disclosure. This may be different for officials in a lower grade, mostly less used and less likely to be exposed to public attention. A more restrictive approach would therefore be appropriate in those cases.

Is disclosure allowed according to the data protection legislation?
The extent to which the privacy of the data subject may be substantially affected determines the need to analyse of whether disclosure would be allowed according to data protection legislation.

Here it becomes important that the institution has a clear policy - laid down in internal rules and well communicated to its staff - on how to deal with similar matters. In the absence of such a policy, it is quite likely that the publication of a specified list covering staff members of all grades would be incompatible with the purpose for which these data have been collected and therefore would infringe Article 4 of the data protection regulation.

Conclusion:
This example shows that personal data of the institutions' staff are protected by the principles of the data protection regulation. However, some personal information could still be made publicly available in certain cases, depending on the nature of the data and other circumstances of the case which make it proportional and in accordance with fair and lawful processing.

Example 6: Should a list of applicants for the post as director be published?

In a specific case, the general information provided to the candidates when the post was published stated: 'The Director will be selected and appointed [...] according to selection and recruitment procedures'. No further written information was provided to candidates. During the recruitment procedure, only candidates who were short listed received information about the other people on the list.

Comment:
Is the privacy of the data subject at stake and is the data subject substantially affected?
The general rule of thumb is that the mere act of disclosing the name of a person does not affect his or her privacy, especially not if it concerns officials of a public body acting in a public capacity. This particular case relates to access to the names of the applicants for a specific high-level post. And, as has been stated previously, in the case of recruitment procedures, certain employees may be subject to disadvantages from their current employers or suffer otherwise should it be known that they have applied for another post. Confidentiality is an important part of the selection procedure although it has to be balanced with the public interest of accountability at the time of recruitment.

In this case the candidates were not informed about public access at the time of collection of their personal data and, importantly, were not given the possibility to justify why they should be exempted from disclosure. As disclosure could substantially harm the data subject, it can not take place without consultation with the applicants, so as to get consent, or at least hear their view on the consequences of possible disclosure.

Is disclosure allowed according to data protection legislation?
Public disclosure must be seen as conflicting with the purposes of collection of the data (Article 4). Naturally, the candidates have not given consent, as defined in Article 2 (h) for public disclosure, nor could they have reasonably understood that their names would be made public. The only disclosure that can be justified and legitimate is to reveal the names of the short-listed names to those who made it to the list. That guarantees some level of accountability and transparency in the selection process, which can be considered necessary for the performance of the public task involved as required in Article 5 (a).

Just as in other examples regarding recruitment procedures, the public interest in disclosure is reinforced by accountability reasons. It is therefore advisable to inform the candidates better in advance, in a way similar to EPSO procedures (example 2). That allows candidates to provide reasoned grounds for why he or she would be substantially affected by, and should be exempted from, public disclosure.

Conclusion
This example clearly shows how data protection principles can serve to protect the interests of the persons concerned and - at the same time - encourage a transparent recruitment process.

Example 7: Can the external activities of officials be made public?

A newspaper requested access to a register of approvals given for external activities of officials of an institution. It was advocated that the register should only be supplied once the names of the officials concerned had been deleted; only partial access was granted to the list. That solution was however considered transitory and officials will in the future be informed that this type of document may be disclosed.

Articles 12 (a) and 12 (b) of the Staff regulations cover a wide area of private and public activities. Applied strictly, all types of more organised and structured engagements outside of office-hours would need to be included in the register. A less strict application could lead to include only paid or otherwise (public) functions, such as high-level participation in an NGO or being member of the board of a private company.

Comment:
Is the privacy of the data subject at stake and is the data subject substantially affected?
Public officials must be aware of the public interest in information relating to their working capacity and possible conflicts of interests. This means that 'at work' reasonable expectations of privacy must be different, at least to that extent. However, external activities may be quite different in nature. It is therefore difficult to draw a general borderline on whether disclosure would involve the privacy of the officials. It is clear that privacy is increasingly concerned when it comes to free-time activities of an official of a private nature, and even more so if this would involve sensitive or confidential data (as elaborated in section 4.3.3, second paragraph). The fact that a certain official is a member of the board of a tennis club, or that he is active in a church or a charitable organisation involves his private life, and his privacy could be substantially affected by public disclosure. On the other hand, the general rule of thumb must be that information on paid or otherwise public functions of public officials have little privacy implications and shall be made public.

As the list may contain other information than on paid or otherwise public functions, and as the privacy aspect will vary from one entry to another in the register, disclosure must be based on a case by case analysis. This will allow for a determination of the degree of privacy

involved in each entry (unless that would result in an unreasonable amount of administrative work (see 4.2.3)). That type of consideration has to reflect the high profile nature of the topic and the public interest in accountability and credibility. The data subject would, in general, be considered to be seriously affected by disclosure of information that relates to membership of political organisations or other sensitive data, such as defined in section 3.4.4.

Is disclosure allowed according to data protection legislation?
This type of list contains information on employees that have another source of income and/or that have a risk of conflict with their function. The collection of such data can be considered necessary for the performance of a public task or for compliance with an obligation in the Staff regulations. There is also a strong public interest in full disclosure, and preserving the integrity of a public office is an integral part of the public task. However, this requires a careful judgment of responsible authorities as well as a clear and timely communication of applicable rules and policies to employees before they are asked to provide the relevant information, to make any disclosure compatible with Articles 4 and 5. Sensitive data in the sense of Article 10 must, in general, not be disclosed.

In cases where, because the privacy harm to the data subject is substantial, it is deemed disproportional to grant full access, the possibility of partial access needs to be considered. Any deleting of references to officials whose privacy would be infringed according to the 4 (1) (b) exception must be motivated on a case-by-case basis. In most cases, partial access would not give the same result as full access and it needs to be limited to what is necessary.

Conclusion:
This is a typical example where the controller can easily help to promote public access and data protection by providing the data subjects with information on the possibility of public disclosure at the time of collection of the information, within the limits imposed by principles of fair and lawful processing. It could also be stipulated in internal rules. The controller should also provide the data subjects with the possibility to opt-out of disclosure on reasonable and valid grounds.

Example 8: Can contact details of officials / the Who's who of an institution be published?

To date, most institutions make public personal data such as name, position and office phone number of officials who hold a higher or more public post. In some cases, the same information is disclosed through the website of an institution down to desk officer level.

Comment:
Is the privacy of the data subject at stake and is the data subject substantially affected?
In general, disclosure of name, office number, area of responsibility, etc. of a public official has little privacy implications. This is another example which highlights the need for civil servants of a public body to be aware that they are subject to a higher degree of transparency than if they worked in the private sector. Therefore, the general rule of thumb is that such information can be made available without infringing the privacy and integrity of the individual. Only in cases such as where the official has previously been exposed to threats, should he or she have the possibility to be exempted from the list - disclosure will not substantially affect the data subjects in other cases. There is therefore no need to go into an analysis of whether disclosure would be allowed according to data protection legislation.

Also this type of case would be helped by a proactive approach, in which the publication is announced along with the possibility to opt-out on compelling and legitimate grounds. As mentioned before, this approach will have to take data protection principles fully into account.

Conclusion
This example clearly demonstrates that a reasonable approach to the publication of contact data of officials will not run into legal problems. It should be noted however that some prudence is still needed to avoid undue 'side effects' like frequent interruptions at work, or 'spamming' in the case of e-mail addresses.

Example 9: Can an attendance list, the minutes of a meeting or a list of officials who are in a selection committee be made public?

The participation of someone in a meeting on behalf of an institution or a private company may lead to processing of personal data in the sense that the attendance list may be made public. Another such example is a list of officials being part of a selection committee.

Comment:
Is the privacy of the data subject at stake and is the data subject substantially affected?
In general, there is little privacy in the examples above. There is no such thing as a general right to anonymity for public officials - partial, or no access has to be motivated with reasonable and valid grounds. The fact that, for instance, the names of participants to a meeting within the consultative role of the Committee of Regions are made public through an on-line meeting protocol has little implications on the privacy of the people involved, as they are there in a public capacity representing not themselves but, for example, their employer or their constituency. The general rule of thumb is to allow for full access, while providing people with the possibility to be exempted from disclosure if they have compelling and legitimate grounds. A data subject who does not provide reasons for being exempted from disclosure can not be considered to be substantially affected by it. As the privacy of the data subject (in general) is not substantially affected, there is no need to go into an analysis of whether disclosure would be allowed according to data protection legislation.

However, there are specific situations in which this rule can not be applied automatically. In a current case before the Court of First Instance Justice, the Bavarian Lager Company wants the Court to annul the decision of the Commission to not disclose the full version of the minutes of a meeting at DG Internal Market between representatives of the Commission, the UK government and breweries. The meeting dealt with market access in the UK and Bavarian Lager wanted the Commission to reveal the identity of certain persons whose names had been blacked out in the version they received. An argument for not disclosing could be a potential risk to the Commission's ability to carry out investigations, should it be forced to reveal the identity of persons giving information. This could be an instance of point [B] of the check-list. The case is pending before the Court of First Instance, so we will not comment upon it.

Conclusion
This example shows that - as a rule - privacy and data protection considerations play a limited role in this context, and other aspects may be more relevant.

Example 10: 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. The list sorts the MEPs 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 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?

The political opinion of a data subject is categorised as sensitive data (Article 10) and is intrinsically linked to the privacy of the person. As was stated in section 4.3.3, 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.

Is the data subject substantially affected by disclosure?

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. In some cases, the assistants even work publicly for the same party. However, in specific cases (such as more extremist parties), disclosure could substantially harm the data subject. It is important that assistants have a possibility to be excluded from the list, should they provide compelling and legitimate reasons for it. That could enhance and promote compliance with both regulations.

Is disclosure allowed according to data protection legislation?

The publication of the name of a person on the list of accredited assistants is in conformity 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 special categories of data, such as personal data revealing political opinions. However, the article is not absolute - important exceptions are laid down in Articles 10 (2) and (4).

In relation to the exceptions of Article 10, one must be aware that consent, in accordance with Article 2 (h), is not collected prior to disclosure. On the other hand, the act of working as an assistant to a MEP comes, in some sense, close to the notion of participating actively to the public politics in a democratic society. Although this data has not been 'manifestly made public' in general, disclosure is allowed if appropriate safeguards are provided and if there is a substantial public interest. In view of the purpose and the content of the list, there is such a substantial public interest and it is therefore proportionate to disclose the list.

Conclusion

This example shows that a general policy promoting a high degree of publicity, even in the case of 'sensitive data', may be acceptable in practice, provided that such data are relevant in the specific context and adequate safeguards are available for exceptions on legitimate grounds.

Example 11: Can a list of trainees at an institution be made public?

In the case of the 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 privacy. When signing the application form for a traineeship, 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 the Internal rules, which concerns the admission procedure, expressively states: 'the results of the selection procedure will not be published'.

Comment:

Is the privacy of the data subject at stake and is the data subject substantially affected?

In general, disclosure of information such as the names of people (who most often just finished 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. The applicants should therefore be given the 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 in this case imperative to keep in mind that the candidates were given explicit information that their personal data would not be revealed. Disclosure would therefore run contrary to the reasonable expectations of the data subjects. In spite of the strong case for public access, notably for reasons of accountability according to Article 5, public access can not be granted under these circumstances.

Conclusion:

This is in effect a case in which public access could not be granted due to the drafting of the internal rules - despite the fact that the personal data concerned have little privacy implications in most cases. A proactive approach, in which the internal rules are amended so that the candidates are informed that if they accept a traineeship, their names will appear on a list which will be disclosed to the public (in combination with a possibility to opt-out on compelling and legitimate grounds) would be a much better solution.

6. Check-list

6.1. Introduction

This check-list is a simplification of the contents of the previous chapters. The aim is to guide officials who deal with the question whether or not to disclose a specific document containing personal data. One should keep in mind that disclosure may necessitate a contact with other officials, such as the controller or the data protection officer, so that they are aware that the data are made public.

As was stated under heading 4.3.2: once it has been determined that a document falls within the scope of the public access regulation (or a similar legal instrument) [A], and no other provision prohibits access [B], that it contains personal data and that it is a third party asking for access to it [C], the decisive question is: does the exception of Article 4 (1) (b) apply?

The following three conditions were set up, all of which need to be fulfilled as to enable the 4 (1) b exception of the public access regulation to apply:

[D]. Is the privacy (and integrity) of the data subject at stake?
[E]. Is the data subject substantially affected by disclosure?
[F]. Is disclosure allowed according to data protection legislation?

6.2. Check-list

[A] Applicability of the public access regulation?

1) Does the document fall within the scope of the public access regulation?
[Reg. 1049: Art. 1 (a), 2 (1) -2 (3), 3 (a)]

2) Does the document fall within the scope of other similar legislation, with the same type of exception related to privacy and integrity of the individual, such as the decision on access to documents established by the Court of Auditors?

Guiding elements: documents (any content whatever its medium) drawn up or received by an institution fall within the scope, which, also, covers all areas of activity of the EU.

[B] Do other provisions prohibit public access?
[Reg. 1049: Art.4 (1) (a), 4 (2) - 4 (5)]

Guiding elements: If the document concerns: – public security; – defence and military matters; – international relations; – the financial, monetary or economic policy of the Community or a Member State; – 'space to think'; – court proceedings and legal advise; – investigations and audits, etc.

disclosure may be hindered by other provisions.

[C] Does the document contain personal data? Who is asking for access to it?

1) Does the document contain personal data?

[Reg. 45: Art. 2 (a)]

Guiding element: Public access can naturally not be refused on the 4 (1) b grounds if the document contains no personal data.

2) Who is asking for the document?

[Reg. 45: Art. 2 (a), 2 (f/g), (8 - 9), 13, 17]

- The data subject? [Reg. 45: Art. 2 (a)]
- Third party? [Reg. 45: Art 2 (f/g)]

Guiding elements:
- If the data subject asks for disclosure, access can not be refused on the 4 (1) b grounds as he or she will exercise the right to access to personal data (Article 13). In such cases, the data subject is likely to be in contact with the controller (not the official handling a request for public access). This is also the case with the right to notification to third parties (Article 17).
- The public access regulation is in general not applicable if the recipient is located outside the EU. But when access is granted in such cases, Article 9 of the data protection regulation will be applicable.

[D] Is the privacy (and integrity) of the data subject at stake?

[Reg. 45: Art. 2 (a); case law interpretation of privacy and integrity]

- What type of personal data is involved?
- In which context do the personal data appear?
- How were the personal data collected?

Guiding elements:
- The fact that a document contains personal data [Article 2 (a)] does not automatically invoke the 4 (1) b exception. Personal data must be distinguished from privacy.
- Privacy concerns private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially.
- The notion of private life does not exclude activities of a professional or business character.
- At the same time, public officials must be aware that their personal data may be of public interest for legitimate reasons such as accountability and transparency. The more public the function of an official is, the more the public can have a legitimate interest is to be informed about the official.
- The privacy notion does not always extend to people acting in a public capacity.

[E] Is the data subject substantially affected by disclosure?

Guiding elements:
- 'Substantially affect' implies that there is a degree of harm to a legitimate interest of the data subject.
- This condition is more likely to be fulfilled should sensitive data be disclosed.
- Disclosure, even of 'innocent' personal data, such as the address or the name of the data subject may, in certain cases, seriously affect him or her.
- In particular cases, it is justified to contact the data subject and receive his or her opinion on what effects disclosure would have. The opinion of the data subject should be one part of the analysis; it can in no way substitute it.

[F] Is disclosure allowed according to data protection legislation?

Guiding elements:
- The primary source of legislation is the data protection regulation. In order to establish whether its principles are infringed, a number of key articles to be mentioned hereafter need to be analysed.
- Importantly, exception 4 (1) b can only be invoked if the data protection regulation explicitly prohibits disclosure.
- Two key considerations that need to be kept in mind when analysing whether the 4 (1) b exception should apply are: the principle of proportionality and the principle of the right to information.

1) Is the personal data processed in a way incompatible with the purposes for which they were collected?

[Reg. 45: Art. 4 (1) (a), (b)]

- The purposes are determined at the time of collection.
- How could the data subject reasonably understand the purposes?

Guiding elements:
- If the data subject was informed about the possibility of disclosure at the time of collection, the 4 (1) b exception is unlikely to be applicable. He can be informed by supporting documents (directly or indirectly referred to at the time of collection) laying down the possibility of granting public access to the personal data.
- If the data subject has been informed that his or her personal data will not be subject to public disclosure, the exception is likely to be applicable.

2) Would disclosure be necessary for the performance of a task carried out in the public interest on the basis of the EC Treaties or other legal instruments adopted on the basis thereof? Is it necessary for compliance with a legal obligation?

[Reg. 45: Art. 5 (a), 5 (b); EC Treaty 255; Reg. 1049]

Guiding elements:
- Most of the institutions and bodies are legally obliged to grant the public access to documents.

– 'Public interest' must be interpreted in the light of the importance that the European Council has attributed to transparency as well as to the principle of the right to information.
– As a result, in most cases, when a decision has to be made on the access to certain public documents, both Article 5 (a) and 5 (b) of Regulation 45/2001 could be invoked, since disclosure would normally be deemed necessary in the public interest as well as to comply with a legal obligation. The distinction between the two grounds for granting public access is quite theoretical. A practical recommendation is to contact the data subject when there is reason to believe that his or her privacy is substantially affected, so as to get his or her opinion on the consequences of disclosure.

3) Has the data subject already unambiguously given consent for disclosure?

[Reg. 45: Art. 2 (h) and 5 (d); supporting documents]

• Was consent obtained implicitly or explicitly, in a way avoiding any ambiguity?
• Was consent obtained voluntarily and after adequate information?

Guiding elements:
– The degree (and value) of consent needs to be evaluated on the basis of how it was obtained.
– Informed consent can be obtained by a reference to a different document.
– If the data subject has given consent for disclosure, it can not be refused on the grounds of Article 4 (1) (b).

4) Are the personal data of a sensitive character?

[Reg. 45: Art. 10]

Guiding elements:
If the personal data concerns any of the following categories, Article 4 (1) (b) would prevent disclosure (unless any of the exceptions to Article 10 applies):
– racial or ethnic origin;
– political opinions;
– religious or philosophical beliefs;
– trade-union membership;
– health or sex life.

5) If the data are sensitive, would there be an exception to the prohibition of processing?

[Reg. 45: Art. 10 (2) and 10 (4); Reg. 1049]

• Has the data subject given an express consent?
• Has the personal data been manifestly made public by the data subject?

Guiding elements:
If the data subject has given consent, or if he or she has manifestly made public the personal data, then disclosure can not be hindered by reference to article 4 (1) (b).

6) Would disclosure infringe the rights of the data subject?

[Reg. 45: Art. 13, 17, 18]

- Does the data subject need to be informed about the disclosure?
- Does the data subject have compelling legitimate grounds relating to his or her particular situation to object to disclosure by virtue of the 'public interest'?

Guiding elements: In order to be able to comply with the rights of the data subject, the controller may need to be informed about disclosure.

7) To what extent is disclosure of the personal data a proportionate measure?
The final step is the proportionality test. The following (non-exhaustive) list of questions provides guidance:

- What kind of harm would disclosure lead to?

Guiding elements: – It is important to concentrate on the actual harm that disclosure would do to the data subject. All aspects of Article 4 (1) b must be part of the analysis. – The data subject needs to be substantially affected for disclosure to become a disproportionate measure. The situation of the data subject and the potential consequences of public disclosure for him or her must be taken into account. – In no case should disclosure have as a result that a private person is deprived of, or unduly restricted in his fundamental right to data protection.

- Will the information be published, or 'only' handed over to the applicant?

Guiding element: The strain on the privacy of the data subject is naturally less, should the document 'only' be handed over to the applicant, and not made public on, for instance, the website of the institution.

8) If it is disproportionate to disclose the full version of the document, would partial access be a solution?

Guiding elements: – Partial access or anonymisation is an exception to the general rule of full access. – Partial access is a practical solution if the harm to the privacy of the data subject is substantial and if the personal data in question is not the primary source of interest for the public. The aim is to reduce the privacy harm to an acceptable level. – Partial access is given by solely deleting the elements of the text that cause the substantial harm. – If the administrative work related to the granting of partial access would be of an unreasonable amount, the applicant for the document shall be contacted in order to find a solution. The 15 day delay can also be extended if needed..

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