COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 15 November 1988

CJ-PD-GT/11 (88) 20

WORKING PARTY No. 11

of the Committee of experts on data protection
(data protection and freedom of information)

The interaction between freedom of information legislation and data protection legislation in Europe

Study prepared by
Mr. Herbert BURKERT
(Cologne, Federal Republic of Germany)

THE INTERACTION BETWEEN FREEDOM OF INFORMATION LEGISLATION AND DATA PROTECTION LEGISLATION IN EUROPE

[DRAFT][1]

Herbert Burkert[2]

1. Introduction into the problem area

Example 1: R wishes to access data relating to him stored electronically at a public authority. Data protection legislation entitles him to such access. There is also freedom of information legislation[3] in this country. This freedom of information legislation is also applicable to electronically stored data. This includes personal data in general and thus personal data relating to R. The exemptions to accessing one's own data in data protection legislation, however, give the administration a larger discretion to refuse access than the exemptions in freedom of information legislation to access personal data.

Example 2: R wishes to access data relating to him stored electronically at a public authority. Data protection legislation entitles him to such access. There is also freedom of information legislation in this country. With regard to accessing personal data this freedom of information legislation is only applicable to data in traditional paper files. R can only use the data protection act for his request. The exemptions of the data protection act apply. His request is refused. Had the data been in a traditional file he could have used the freedom of information act where the exemptions are less strict, and access would have been granted.

Example 3: R wishes to access data relating to him in a traditional paper document. There is only a data protection law in his country. This law is only applicable to electronically stored data. If his data were stored electronically R could have accessed it because none of the exemptions in the data protection law would have applied.

Example 4: R wishes to access personal data relating to S stored electronically at a public authority. There is freedom of information legislation in this country which entitles R to access electronically stored information held by public authorities. This includes also personal information and thus personal

---

1 It should be noted that there has been no opportunity yet to check references to national legislations in this text with up-to-date submissions by the Member States to the questionnaire. Further information and comments will be made, as within my capacity, at the presentation and in the course of the meeting.

2 Attorney at Law, Cologne Bar, and Senior Researcher at the Research Center on the Information Economy, Gesellschaft für Mathematik und Datenverarbeitung, Cologne, Federal Republic of Germany. The views expressed are solely those of the author and are not attributable to any other source.

3 In the text "freedom of information" is used instead of "access to official information" because data protection legislation also contains access clauses. It is agreed, however, that "freedom of information" may give cause to other misundertsandings; it is, however, a terminology which has reached some diffusion.

information on S. There is also data protection legislation in this country. While this legislation only entitles requesters to see their own information, it does not exclude the communication of personal information to third parties in general, but sets up conditions on availability which are very strict. The freedom of information legislation also contains restrictions on accessing personal information. These restrictions, however, are formulated in an "access friendly" way.

Example 5: R wishes to access personal data relating to S stored in a paper document at a public authority. There is freedom of information legislation in this country which entitles R to access information held by public authorities. This includes personal information and thus personal information on S stored in paper files. There is also data protection legislation in this country. This data protection legislation contains strict regulations on the availability of personal information. This data protection legislation, however, is only applicable to information stored electronically or in a systematically retrievable way and is therefore not applicable. The freedom of information legislation also contains restrictions on accessing personal information. These restrictions, however, are formulated in an "access friendly" way. Should S be less protected only because his data is not yet stored electronically?

Example 6: R wishes to access personal data relating to S stored in a public register. There is no freedom of information legislation in this country but the special legislation relating to that register entitles R to access the information. The register is modernized and now kept electronically. The legislation has remained unchanged from the days when this register was kept as paper documents. There is also data protection legislation in this country. This data protection legislation contains strict regulations on the availability of personal information . Is solely the legislation relating to the register to be applied because it might be regarded as more specific? Should not the interest of S be reconsidered by at least applying the principles of the data protection legislation in interpreting the register law, since the register has changed with regard to the storage medium?

These examples, which we have used to introduce the scope of the problems, are not merely theoretical. They do not even represent all possible interactions between data protection and freedom of information. They suffice, however, to show that at the present stage there are problems with coherence. This has, at least partly historical reasons. Data protection legislation and freedom of information legislation have developed in an uncoordinated manner, because they have been regarded as different responses to different problems. Freedom of information has been considered as an additional safeguard for administrative accountability. Data protection, mainly a reaction to a technological development, has tried to maintain personal identity in the face of new power potentials of this development. Now freedom of information gradually is adapting to technological change as well by including electronic storage media in its reach of application. Even where there is only data protection legislation so far, the need for an freedom of information supplement has been realized:

> "[Effective and convincing data protection] can only be achieved if data protection is seen as part of a comprehensive confrontation with the conditions of access to information and its distribution within a

democratic society. Data protection and freedom of information are therefore not opposites, but different parts of a composite whole."[4]

Although not all Council of Europe Member States have yet enacted both sets of legislation[5], this is a situation which the legal instruments of the Council of Europe, the Convention[6], the Recommendation (81) 19 of the Council of Ministers[7], and the Recommendation 1037 (1986) of the Parliamentary Assembly point to. Consequently, there are two needs

a) to supplement each of the legislations by the other, and

b) where this has already happened or where this is going to happen, to master their interactions.

It is the purpose of this paper to contribute to b) and to the task "to identify criteria and principles according to which data protection and access to official information could be reconciled"[8] against the background of the work already undertaken at the 1st meeting of the CJ-PD-GT-11[9].

Three main problem areas need further attention:

Since both data protection and freedom of information legislation address access to personal information (data protection mainly to grant access to the requester to his own data and to restrict its general availability; freedom of information mainly so as not to exclude it from principle availability, but nevertheless safeguarding the interests of privacy), it seems as if problems might be solved by clearly separating the application areas by reference to e.g. storage media (see part 2). But even if such separation would be successful (and even more so where there is no such separation) there is still the question how to ensure that there is coherence in the way data protection and freedom of information considerations are balanced. Special considerations might be necessary when a requester is seeking access to his data (part 3) and when he is seeking access to somebody else's personal data (part 4). In

---

4 Simitis 1986, 42.

5 The following have both data protection and freedom of information laws: Denmark, Finland, France, Norway, Sweden; just freedom of information legislation is to be found in the Netherlands, just data protection legislation in Austria, Germany, Ireland, Luxembourg, United Kingdom.

6 Council of Europe: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg. 28 January 1981.

7 Recommendation R (81) 19 of the Committee of Ministers to Member States on the Access to Information held by Public Authorities , adopted by the Committee of Ministers on 25 November 1981.

8 Recommendation 1037 (1986) of the Parliamentary Assembly, No. 13 a.

9 Working party no. 11 (freedom of information and data protection) of the Committee of Experts on Data Protection , Strasbourg 27 - 29 January 1988) CJ-PD-GT11 (88) 6.

view of the complexities of the issues the paper will provide a personal, concrete proposal where, in an exemplary and practical manner, further analysis might be useful (part 5).

General freedom of information issues would certainly deserve more attention, in particular since there have been new interesting developments since the Council of Europe recommendation in this field. Furthermore, a general understanding, particularly of the applicability of freedom of information legislation is necessary in order to discuss potential conflicts with data protection. Also, other issues, related to both freedom of information and data protection would deserve further attention, like e.g. archive legislation, as one of the areas of special sector legislation, where both transparency and privacy issues play an important role. Nevertheless, due to its specific restraints, this paper will deal with the interactions of data protection and freedom of information legislation only. In view of the current state of legislation in Member States, examples will also be taken from other countries which have both sets of legislation.[10] But these problems are not only of current interest to those countries (cf. Example 6 which is taken from a current debate in Germany[11]). Finally, while the Parliamentary Assembly uses the term "official information" this paper will use the term "public sector information", staying thus closer to the Recommendation R (81) 19 which uses "information held by public authorities".[12]

2.Separating the areas of application

If the interactions between data protection and freedom of information are problematic, would it not be possible to restrict these problems by clearly separating the areas of application? Such attempts are being made:

---

10 Such legislation may be found e.g. in Canada both on the federal and provincial (Quebec, Ontario) level, the United States and to some extent in Australia (where the federal access legislation also contains a right to correct data relating to the requester).

11 Cf. the current debate on the companies'registers ("Handelsregister"): Kollhoss 1988. Although in the German context data protection is restricted to physical persons the conflict is relevant for such registers since they not only include information on legal persons.

12 The term "official", in the view of the author, also seems to carry certain restrictive implications, like e.g. some prior authorization, or, seems to connotate a specific stage of a document (in contrast to a "draft" e.g.).It is, however, the approach of freedom of information legislation, to consider in principle all documents in the public sector as possible objects of the legislation, defining then, within the laws, such documents to which the law might not apply or to which only specific regulations might apply. This approach makes the inclusion or exclusion a point of law, to be tested in the courts. It is agreed, however, that the definition used here is itself not without problems, because the extension of the public sector is different in different countries and not all institutions or organizations of the public sector might be covered. One notable exemption e.g. are the courts in their judicial functions which are usually excluded from the applicability, either because they are not regarded to be part of the administration proper, or because of avoiding conflicts with specific procedural law which usually covers the accessibility of court material, or to guard the secrecy of judicial deliberations.

Example 7: In Denmark e.g. registers and systematic collections which are processed electronically are exempted from the access right in the freedom of information legislation[13] , with exception of such electronic registers which provide inventories of documents[14] . Possible "lacunae" which might develop with regard to access to electronic storage media which are not covered by the data protection act covering the public sector might eventually be regulated by specific regulations which would also cover the cost of access to such registers[15].

Example 8: In France e.g. the question of data protection or freedom of information applicability (for accessing one's own data) is mainly solved by reference to the way the information is organized which the requester wishes to see. As long as this information is in a "fichier"[16] (whether manual or electronic) only the data protection access regulations apply.[17] Should the document not be in a "fichier", only the access provision of the freedom of information applies, which only knows access of the person "concerned"[18].

Example 9: In the US the Privacy Act is only applicable to "records", where as the Freedom of Information Act does not know such a restriction.

These examples already indicate a trend in the current state of legislation: Data protection access is mainly concerned with access to computerized data. Some legislations, however, it should be remembered from the data protection analysis undertaken in the Council of Europe, allow access to systematic collections of data or even include manual files. Freedom of information legislation has mainly been concerned with traditional (paper) documents, but lately also includes automated recordings.

Although some countries have tried to make a separation between freedom of information access and data protection access to personal information in relation to the storage medium and/or the way in which the information is organized, such attempts do not exclude per se areas where both acts would be applicable at the same time. Differentiations according to storage media seem to suffer from additional disadvantages. They involve further specifications of terms like systematic recording, record or "fichier"; they lack transparency for the user (and the administration as well which has to implement coherent information management strategies); they are only of temporary value: once the administrations will extend electronic filing beyond personal registers, computerized storage will generally have to be covered by freedom of information laws so as to maintain their efficiency. Finally the problem of coherence is not solved: Even if data protection and freedom of information

13 § 5 (2) Lov om offentlighed i forvaltningen, Lov nr. 572 af 19 december 1985.
14 Described in § 5 (1) no.2 of that law.
15 § 5 (3).
16 About the problems of defining "fichier" cf. CADA 1986, 11.
17 CADA 1988, 38 with reference to the interpretation by the Conseil d'Etat.
18 Cf. also Lasserre et al. 1987, 106ff.

are kept separate, efforts must be made to ensure that in both areas balancing of interests in protection and in disclosure takes place according to the same principles. Differentiations of this kind will therefore not spare us from the necessity to address the interactions more closely:

3.Interactions concerning access to one's own data

Data protection access is mainly concerned with access to personal data relating to the requester; freedom of information access is not restricted to personal data but does not exclude -in principle- access to personal data and could thus also be used by the requester who wishes to see his own data.

With regard to restrictions on access to personal data we observe regulations in data protection legislation which restrict the access of the requester to data relating to himself (apart from those which restrict the availability of personal data to third parties, cf. infra part 4). These exceptions usually refer to such data which has been collected on the requester (rather than provided by himself) or which is the result of an analysis. The reasons for such restrictions fall under those categories as described as possible derogations from the data protection access right in Art. 8 (2) of the Convention.[19]

Restrictions in the context of freedom of information legislation only deal explicitly with access to other people's personal data. These restrictions, in the context of freedom of information, are only part of a set of other restrictions which are summarized in Recommendation R (81) 19 Appendix V[20]. Some countries have foreseen additional procedures, in analogy to the individual consent principle in data protection, which involve the data subject in the decision making by the administration on the release.

How can coherence between these restrictions be achieved?

---

19 "Derogation shall be allowed (...) when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of : a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; b. protecting the data subject or the rights and freedoms of others." Note also the exemptions in Art. 8 (3) of the Convention with regard to statistics and for scientific research purposes "when there is obviously no risk of an infringement of the privacy of the data subjects."

20 "(...) as are necessary in a democratic society for the protection of legitimate public interests (such as national security, public safety, public order, the economic well-being of the country, the prevention of crime, or for preventing the disclosure of information received in confidence), and for the protection of privacy and other legitimate private interests, having, however, due regard to the specific interest of an individual in information held by the public authorities which concerns him personally."

Example 10: It had been in the US where the problems concerning the access of the requester to his own data in the context of both data protection and freedom of information legislation had caused quite some problems[21]: If the requester accesses his personal which is not in records as defined in the Privacy Act, the situation is simple: only the Freedom of Information Act applies since the Privacy Act only regulates personal data in records ; this is the "media/file organization" dividing line described above (example 9). If, however, the personal data is in a record, both acts would apply. 552 (a) (q) (1) of the Privacy Act therefore regulates that if a requester could access his own data according to the Privacy Act as well as the Freedom of Information Act (FOIA) , and if the FOIA exempts that information from access but the Privacy Act does not, then the Privacy Act applies. If, however, access (to one's own data) is permitted by the FOIA (the exemptions there are more precisely and restrictively formulated) but exempted by the Privacy Act (where the exemptions a more broadly formulated) the situation had been open to interpretation, because the FOIA (by its third exemption) refers to other statutes which might contain exemptions and thus refers back to the Privacy Act.[22] The situation, however, now seems to be clear since the section 552 (a) (q) in the Privacy Act reads now in total[23]:

> "(1) No agency shall rely on any exemption contained in section 552 of this title [Freedom of Information Act , H.B.] to withhold from an individual any record which is otherwise accessible to such an individual under the provision of this section [of the Privacy Act, H.B.].
> (2) No agency shall rely on any exemption in this section [the Privacy Act, H.B.] to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title [the Freedom of Information Act, H.B]."

The solution in this example points to a general solution which might be considered in the Council of Europe context: Looking at existing Council of Europe instruments we find that the exemptions both with regard to data protection and freedom of information are similar (cf. Art. 9 (2) of the Convention and Appendix V to the Recommendation (81) 19). In case that freedom of information access restrictions are more limiting the Recommendation already points out that there should be :

> "(...) due regard to the specific interest of an individual in information held by the public authorities which concerns him personally."

This principle could be extended to the case in which the data protection restrictions are more limiting: In that case due attention might be paid that the interest of the individual in accessing his own data should not be more restricted than by the conditions set in freedom of information regulations.

---

21 Cf. Marson/Adler 1988b, 234ff.

22 These complications at that time were one of the motives for the Canadian legislators to seek a comprehensive and coherent approach to freedom of information and data protection.

23 Amended 1984 by Public Law P.L. 98-477, 98 Stat. 2209.

4.Interactions concerning access to other people's data

Data protection legislation does not contain access rights to other people's data; it may contain restrictions on the availability of such data. This, however, does not exclude that the administration may communicate personal information to third parties (or other parts of the administration). Such communication usually is admissible with the consent of the data subject, if required by law, if necessary for the fulfillment of lawful purposes of the requesting party, and/or after a balancing test between the interests of the data subject and the receiver. There may be further restrictions, as e.g. the need to substantiate the interest in obtaining the data and certain conditions on reuse imposed on the receiving party.[24] Freedom of information legislation does not make a difference between accessing one's own and other people's data. It, however, also contains safeguards for personal privacy. Again, the question of coherence arises:

Example 11: The US Privacy Act sets up restrictions on the availability of personal information, so does the FOIA. But unlike in the conflict above (where we dealt with the requester's right to his own data) the legislative solution is quite clear: The Privacy Act restrictions are not applicable, if there is a right of access to such information according to the Freedom of Information Act[25]. Problems, however, arise in the interpretation of the relevant exemption of the FOIA according to which are exempted from access: "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." The first question is: what is a similar file. Already at that stage a balancing takes place[26]. E.g. can lists of addresses and names be regarded as similar files ? Now, generally they are regarded to fall under this definition[27]. But this is not sufficient to exempt such files: Access is excluded (only) if such access would constitute a "clearly unwarranted invasion of privacy"[28]. This clause is interpreted as to necessitate a balancing of interests between the public interest in disclosure and the individual's right to privacy. The emphasis is on public interest; so information may be protected if there is no public interest in disclosure[29] but just personal curiosity or an interest merely restricted to commercial considerations.The basic purpose, to be in the public interest, has to be to allow public scrutiny of agency actions:

---

24 Unlike the OECD Guidelines (cf. Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data 1980 : "10. Personal data should not be disclosed, made available (...) except : a) with the consent of the data subject; or b) by authority of law.") the Convention is silent on these restrictions on communication; only indirectly can such principles be derived e.g. from the Art. 5 " a) (...) processed fairly and lawfully; b) (...) and not used in a way incompatible with those purposes; (...)" since "processed", in the definition of the Convention, also includes communication.

25 552 (a) 2 (b) (2) "(...) unless disclosure would be required under section 552 [FOI Act] of this title;"

26 Department of State v. Washington Post Co., 456 U.S. 595 (1982).

27 Manson/Adler 1988, 100.

28 5 U.S.C. § 552(a)(3).

29 As in : Wine Hobby USA Inc. v. IRS, 502 F.2d 133 (3d Cir 1974)(protecting the addresses of home wine makers).

"Conversely, the less disclosure is of interest to anyone but the requester (particularly if the interest is commercial), the less courts are impressed with the public purpose of disclosure."[30]

This requires to look into the interest of the requester although generally the interest of the requester is irrelevant, since freedom of information access is open "to any person".[31] Because of the formulation "clearly unwarranted" the interpretation by the courts in tendency favors disclosure[32]. It is not sufficient that there is a mere possibility of privacy invasion; the production of the records themselves have to lead to the invasion, not the speculations which may rise after the production[33]. Privacy interests relate only to individuals; the information must contain intimate details and be personal. It is regarded to have such qualities, if it may harm the individual or might lead to harassment[34] or retaliation. A prior promise of confidentiality is not relevant. Examples of protected information [35] comprise home addresses of non-union employees, names and addresses of American citizens in foreign prisons because of drug charges, and home wine makers; clearly, generalizations are very difficult to make.

While this solution excludes the considerations in the data protection regulation altogether, it shows that nevertheless privacy considerations re-enter in the balancing test of freedom of information restriction. A more comprehensive approach has been tried in Canada:

Example 12: A solution found on the federal level in Canada points to the usefulness of a comprehensive approach: Data protection and freedom of information are regulated in two separate schedules under one legislative umbrella. These schedules are closely interrelated: Access to personal data (of others) is principally excluded by the freedom of information regulations. Personal information may, however, (inter alia) be accessed under the same conditions as it would be available to third parties regulated in the Privacy Act (which also gives a right of access to one's own data). With regard to personal data the availability exemptions of data protection are thus synchronized with access exemptions in the freedom of information regulations.[36] But the Canadian solution does not exclude the necessity to address balances. In Canada there is a mediating agency for data protection as well as for freedom of information . They may both be involved in commenting on the same access demand to personal data relating to other people's data. It would be interesting to have a closer look at these experiences because by this approach the balancing of protective and transparency considerations is almost institutionalized.

Looking at Council of Europe Member States, we have, e.g. with regard to France, already stated that the relevant freedom of information regulation, concerning personal data, only provides access for the person concerned (and, as it may be remembered, only if the data is not in a "fichier"). It should be noted, however, that the definition of nominative data would nevertheless

30 Mason/Adler 1988, 105.
31 Cf. Edwards 1987, 259.
32 Cf. summary at Marson/Adler 1988, 100ff.
33 Arieff v. Department of the Navy, 712 F.2d 1462 (D.C.Cir. 1983).
34 E.g.: no disclosure of addresses of non-union members to trade unions.
35 Taken from Mason/Adler 1988, 102 ff.
36 Sec. 19 Access to Information Act and sec. 8 Privacy Act.

allow access by requesters to third parties' data which might be called personal in other legislations.[37] Also the definition of " person concerned" is such that access is not absolutely restricted to one's "own" data.[38] If in view of these interpretations a requester is then demanding personal information which has passed this test, then the exemption relating to "le secret de la vie privée, des dossiers personnels et médicaux"[39] has to be tested. But since the access request concerning personal data usually already fails the previous test, mainly because the requester is not the "person concerned", this may be the reason why this exemption has so rarely been applied[40]. It may be added that the freedom of information legislation seeks to exclude diffusion and utilization for commercial purposes of the documents obtained.[41]

These examples suggest that some of the problems might be solved by separating the application areas. But, as already pointed out when discussing the usefulness of such a separation, the problems of coherence remain. Such coherence has to be based on common principles for the accessibility of public sector personal information, taking into account privacy and transparency considerations. Answers to that question might be found rethinking both data protection and freedom of information as parts of one policy on the handling of public sector information.[42] Against this background then a more detailed analysis of the interests at stake would have to take place. Such an analysis, particularly if undertaken on too general a level, would, however, run the risk to remain too broad or to end up in casuistry. It is therefore suggested that an approach might be more useful which looks into a particular application area in order to develop from there an understanding of some general criteria and principles.

---

37 Since the CADA defines "nominative data" :"sont nominatives les informations qui portent une appréciation ou un jugement de valeur sur une personne physique nommément désignée ou aisément identifiable." So e.g. a list of members of a profession is regarded as non-nominative and therefore as accessible by requesters. CADA 1982, 28 f. Cf. Lasserre et al. 1987, 108.

38 Concerned, in the view of the CADA, first of all means that the document has been drawn up with regard to that particular person. But concerned can also mean , that there is a personal and direct interest of the requester in obtaining this document, as e.g. in the context of deceased relatives. Cf. Lasserre et al. 1987, 107.

39 Art. 6 bis , loi du 17 juillet 1978.

40 Cf. CADA 1982, 36. Cf. Lasserre et al. 1987, 112.

41 Art 10 (2) loi no. 79-587 du 11 juillet 1979.

42 Cf. the deliberations of the National Conference of Commissioners on Uniform State Laws in: McCabe 1981.

5.Suggested Area for Further Investigation

Current work on data protection in the Council of Europe points to the necessity to address problems on a sectoral level. It is therefore suggested that a more extensive study is undertaken in one specific area of practical relevance. Such an area has already been addressed by the working party in pointing to the problems of selling personal data which is held by public authorities to third parties, in particular to private sector entities for commercial use or re-use.

This is a problem of reconciling data protection and access to public sector information: such access demands would have to be analyzed according to availability restrictions of data protection as well as according to transparency demands of freedom of information. It is also of growing importance because of economic pressures in the context of developing information markets, particularly among those Member States which are also members of the EEC.

When entering this field the Council of Europe would not enter a field left totally unattended so far. There are countries in which these problems have been realized for quite a while and where these issues are under close scrutiny. The Government of Quebec e.g. is currently addressing this problem in its endeavor to develop a coherent policy with regard to public sector data banks[43]; so have been the US Office of Management and Budget[44] and Council of Europe Member States[45]. Furthermore these issues are being dealt with in the Legal Advisory Board to the EEC GD XIII. Such a task would address the problem of weighing privacy interests and interests in access to public sector information, as well as the particular public interests in the registers or data banks which are at stake.[46] It might consider the various interests to be balanced in such a context, like the interests of the administration (to fulfill its public responsibilities, seeking at the same time to safeguard the flow and the quality of the information by guaranteeing confidentiality, the political interest in as far as such information might reflect upon the efficiency of public policies), the interest of the citizen (who needs public sector information to exercise his political rights, hold the public sector accountable for its activities, who relies at the same time on the confidentiality of information relating to him), the interests of market participants (relying on public sector information, its neutrality and objectivity, to determine business strategies, relying, too, on the confidentiality of their data entrusted to the public sector), the participants in the information market in particular (regarding public sector information as a valuable potential market product to be obtained under favorable conditions and to be sold without undue restrictions). These interests would have to be analyzed against the background of new tendencies: the public sector more and more adapts to information and communication technology; either by economic necessity or because of political intention there are arrangements in which private sector information providers contribute to 'electronic fi-

43 Cf. e.g. McNicoll et al. 1988
44 Cf. the discussion surrounding its Circular A-130 (Management of Federal Information Resources) of December 24, 1985
45 Cf. e.g. in Sweden: Himmelstrand 1986.
46 Cf. Burkert 1987, 177ff.

ling' concepts or elaborate data banks in the public sector; furthermore the public sector realizes the economic potentials of the information it possesses. Also possible repercussions would have to be taken into account if data is collected at the individual's (or where appropriate the legal person's expense) only to see it then "sold" by the administration. Freedom of information considerations continue to play a role after such information has been sold to ensure its further accessibility. Against this background of complex phenomena, minimum requirements for the information flow of personal data between the public sector, the citizen and other private sector parties, in view of both data protection and freedom of information considerations, are strongly needed.

Such an analysis, against the background of our observations under parts 2 to 4, might eventually be able to develop criteria and principles which would allow to balance data protection and freedom of information . As such criteria, which later could be generalized and re-tested, might be taken into account:

- the relationship between the requester and the personal data requested (data relating to the requester/data relating to third parties),
- the extent of the demand (complete file/considerable portions/individual elements),
- the media of the requested material (on-line/tape/print-out),
- the purpose of the request (request in the public interest/for personal use/ for commercial resale),
- the function of the information collected (whether the administration keeps data for public purposes because of the specific confidence put in public administration or wether the information has been accumulated or generated in the execution of its administrative function).

Conditions on re-use (to ensure data quality, the transparency of sources, time and occasion of primary collection) might be considered, as well as cost aspects.

These criteria mentioned here are only of an exemplary nature to illustrate what such an exercise might have to consider without prejudging the outcome of such a task.

6. Summary

The area where data protection and freedom of information interrelate most closely is access to personal information . In principle a requester might access data relating to himself on the basis of data protection legislation as well as on the basis of freedom of information legislation. Where both such legislation is applicable at the same time problems might arise if the exemptions differ in their strictness. Council of Europe instruments and legal regulations as well as laws and administrative practices in other countries seem to indicate that in such cases access which is optimal in the interest of the requester should be granted since the access concerns his own data.

Access to third parties' personal information may lead to conflicts between privacy exemptions in freedom of information legislation (which are usually

formulated restrictively to favor public access) and restrictions on the availability of personal information set down in data protection legislation. Available experiences suggest that it seems to be difficult to arrive at general principles and criteria to solve such conflicts.

Often, conflicts arising from duplicate applications are attempted to be excluded altogether by drawing separations of applicability making the application of either data protection or freedom of information laws dependent on the storage media or the way in which the information happens to be organized. While such differentiation avoids some of the problems encountered by duplicate application, the criteria for differentiation are often difficult to grasp and seem to be -in view of the developments of information technology- only of a transitory nature. Furthermore they do not exclude the necessity to arrive at a general comprehensive approach in balancing data protection and freedom of information principles.

As this, at the present time, might be too general a task, a more precise and sector oriented exercise is suggested by taking the problems of selling personal information by the public sector as an area where to develop "criteria and principles" according to which data protection and access to official information could be reconciled."

References:

Burkert 1987
Burkert, H.: Rechtliche Rahmenbedingungen des Europäischen Informationsmarktes: Zugang zu Informationen im öffentlichen Sektor. Bericht im Auftrag der Kommission der Europäischen Gemeinschaften. St. Augustin 1987.

CADA 1982
Commission d'accès aux documents administratifs: L'accès aux documents administratifs. Deuxième Rapport d'Activité. Paris 1982.

CADA 1986
Commission d'accès aux documents administratifs: L'accès aux documents administratifs. Quatrième Rapport d'Activité. Paris 1986.

CADA 1988
Commission d'accès aux documents administratifs: L'accès aux documents administratifs. Cinquième Rapport d'Activité. Paris 1988.

Edwards 1987
Edwards, M.: Are privacy and public disclosure compatible?: The privacy exemption to Washington's Freedom of Information Act - In re Rosier, 105 Wn 2d 606, 717 P2d 1353 (1986). In: Washington Law Review (62) 1987, 257-275.

Himmelstrand 1986
Himmelstrand, K.: Kommersiellt utnyttjande av myndigheternas datasamlingar. IRI-rapport 1986:6. Stockholm 1986.

Kollhosser 1988
Kollhossser, H.: Handelsregister und private Datenbanken. In: Neue Juristische Wochenschrift 1988, 2409ff.

Lasserre et al. 1987
Lasserre, B., Lenoir, N., Stirn, B.: La transparence administrative. Paris 1987.

Marson/Adler 1988
Marson, Ch.C.; Adler, A.: Exemption 6 FOIA Exemption for Privacy. In: Adler, A. (ed.), Litigation under the Federal Freedom of Information Act and Privacy Act. 13th edition. Washington 1988,97-112.

Marson/Adler 1988b
Marson, Ch.C.; Adler, A.: The Privacy Act. In: Adler, A. (ed.), Litigation under the Federal Freedom of Information Act and Privacy Act. 13th edition. Washington 1988, 219-249.

McCabe 1981
McCabe, J.: Uniform information practices code. In: Information privacy 1981, 248-269.

McNicoll et al. 1988
McNicoll, M., Péladeau, P.,Prémont, M.C.: Implications juridiques d 'une politique de diffusion des banques d'informations gouvernmentales. Groupe de Recherche en Informatique Gouvernmentale. Faculté de droit de l'Université Laval. Rapport remis au ministère des Communications du Quebec. Document de Travail. Janvier 1988.

Simitis 1986
Simitis, S.: Report Working Group 2: Vulnerability of the individual and society. In.: Organization for Economic Cooperation and Development. Information, Computer, Communications Policy. 1984 and Beyond: The Social Challenge of Information Technology. Summary of Conference at Berlin , November 1984. Paris 1986, 40-42.