

DRAFT - April 19, 1999

Frequently Asked Questions (FAQs)

Access

ACCESS PRINCIPLE: Individuals must have [reasonable] access to information about them derived from non-public records that an organization holds and be able to correct and amend that information where it is inaccurate. [Reasonableness of access depends on the nature and sensitivity of the information, its intended use, and the expense and difficulty of disclosing it to the individual].(1) *

*Numbers in parentheses (1-8) refer to endnotes.

1. Q: Is the right of access absolute?

A: Under the safe harbor principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. Nonetheless, the obligation of an organization to provide access to the personal information it holds about an individual is subject to the principle of proportionality and has to be tempered in certain instances. Indeed, the Explanatory Memorandum to the 1980 OECD Privacy Guidelines makes clear that an organization's access obligation is not absolute. It does not require the exceedingly thorough search mandated, for example, by a subpoena, nor does it require access to all the different forms in which the information may be maintained by the organization.

Rather, experience has shown that in responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the request in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with and/or about the nature of the information (or its use) that is the subject of the access request.

Individuals do not, however, have to justify requests for access to their own data.

Expense and burden are important factors and should be taken into account but they are not controlling in determining whether providing access is reasonable. For example, if the information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), then the organization would have to disclose that information even if it is relatively difficult or expensive to provide.

If the information requested is not sensitive or not used for decisions that will significantly affect the individual (e.g., marketing data that is used to determine whether or not to send the individual a catalog),(2) but is readily available and inexpensive to provide, an organization would have to provide access to factual information that the organization stores about the individual. The information concerned could include facts obtained from the individual, facts gathered in the course of a transaction, or facts obtained from others that pertain to the individual. Organizations may deny access to the extent it would reveal confidential commercial information,(3) as defined below, such as marketing inferences or classifications generated by the organization. Where the confidential commercial information can be readily separated from other information subject to an access request, the organization should redact the confidential information and make available the non-confidential information. If an organization determines that access should be denied in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination.

2. Q: What is confidential commercial information?

A: Confidential commercial information (as that term is used in the Federal Rules of Civil Procedure on discovery) is information which an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. The particular computer program an organization uses, such as a modeling program, or the details of that program may be confidential commercial information.(4)

3. Q: In providing access, may an organization disclose to individuals

personal information about them derived from its data bases or is access to the data base itself required?

A: Access can generally be provided in the form of disclosure by an organization to the individual and does not require access by the individual to an organization's data base.

4. Q: Does an organization have to restructure its data bases to be able to provide access?

A: Access needs to be provided only to the extent that an organization stores the information. The access principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

5. Q: The reply to Q1 makes clear that access may be denied in certain circumstances. Are there other circumstances in which organizations would not have to provide individuals with access to personal information they have about them?

A: Yes, although such circumstances are limited and specific. An organization can refuse to provide access to information to the extent disclosure is likely(5) to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where the personal information is processed solely for research or statistical purposes and where such information is not used for significant decision-making about individuals, access may be denied. Listed below are additional examples where access may be denied. This list is intended to be illustrative rather than exhaustive as there may be instances not included here where non disclosure is necessary to safeguard other important countervailing public interests.

Access may be denied to the extent that it would be likely(6) to:

- interfere with execution or enforcement of the law, including the prevention, investigation or detection of offences or the right to a fair trial;
- interfere with private causes of action, including the prevention, investigation or detection of claims or the right to a fair trail;
- involve the disclosure of information that contains references to other

individual(s) and such references cannot be redacted;

- breach an express promise or an implied promise (in contexts where confidentiality is normally expected) that evaluative or opinion material (or the identity of the person who supplied it or both) would be held in confidence;
- breach a legal or other professional privilege or obligation;
- breach a contractual obligation of confidentiality;
- prejudice future or ongoing negotiations, such as those involving company acquisitions; or
- impede sound economic or financial management, including the monitoring, inspection, or regulatory functions connected with such management.

6. Q: Can an organization charge a fee to cover the cost of providing access?

A: Yes. The OECD Guidelines recognize that organizations may charge a fee, provided that it is not excessive. Thus organizations may charge a reasonable fee for access. Charging a fee may be useful in discouraging repetitive and vexatious requests.

7. Q: Is an organization required to provide access to personal information derived from public records?

A: To clarify first, public records are those records kept by agencies of the local, state, or federal government that are normally open to consultation by the public in general. It is not necessary to provide access (or notice and choice) to such information as long as it is kept separately from other information.(7)

8. Q: Does access have to be provided to publicly available information, such as newspaper archives?

A: Because such information is publicly available, it is not necessary to grant individuals' requests for access (or to provide notice and choice) where such information is kept separately from other information. Individuals may obtain access to such information either directly from those organizations that compiled the data or from companies' that are in the business of selling publicly available information by paying the

companies' fee for such access. Where such information is combined with other non-publicly available information, however, an organization should provide access to all such information, assuming such information is not subject to other exceptions.(8)

9. Q: How can an organization protect itself against repetitious or vexatious requests for access?

A: An organization does not have to respond to such requests for access. For these reasons, organizations may charge a reasonable fee and may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.

10. Q: How can an organization protect itself against fraudulent requests for access?

A: An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

11. Q: Is there a time within which responses must be provided to access requests?

A: Yes, organizations should respond without excessive delay and within a reasonable time period. This requirement may be satisfied in different ways as the explanatory memorandum to the 1980 OECD Privacy Guidelines states. For example, "a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests."

Please note: Sector specific access issues, such as those pertaining to pharmaceutical and employee information, will be addressed in separate FAQs dealing with those sectors.

Endnotes

1. The European Commission proposes deleting the words in square

brackets, but could accept alternative wording to show that the right to access is not absolute.

2. The European Commission would prefer wording that makes clear that marketing decisions can be significant and/or involve sensitive information, such as where a decision to send a catalogue depends on the use of sensitive information.
3. The European Commission believes the term "confidential commercial information" is too broad and prefers the concept of "trade secrets" as defined in the Economic Espionage Secrets Act.
4. See footnote 3.
5. The EC believes this standard is too lax.
6. See footnote 5.
7. The EC proposes limiting this text to U.S. public records.
8. The EC would like to see language on publicly available information which avoids creating an exemption that can be used as a subterfuge for avoiding fair information requirements generally and access requirements specifically.