BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Data Processors

Safe Harbor Membership

While the Safe Harbor is a popular data transfer mechanism, the Safe Harbor Principles and other relevant documents do not directly address several important questions regarding Safe Harbor membership. This article examines the implications of Safe Harbor membership for a company that considers itself to be a ''data processor.'' The author concludes that Safe Harbor is a viable data transfer mechanism for data processors that process personal data exported to the United States from Europe.

Membership in the U.S. Safe Harbor Program by Data Processors

BY CHRISTOPHER KUNER

Christopher Kuner is a partner with Hunton & Williams LLP in Brussels. He is the chairman, Task Force on Privacy and Data Protection, International Chamber of Commerce). Kuner can be reached at ckuner@hunton.com. This article a condensed version of an article prepared for the online update of the author's book ''European Data Protection Law: Corporate Compliance and Regulation'' (2nd ed. Oxford University Press 2007).

The European Union Data Protection Directive[1] restricts data transfers to countries outside the EU which are not deemed to have an ''adequate level of data protection.'' One of the best-known mechanisms for providing an adequate level of protection for data transfers to the United States is the so-called ''Safe Harbor'' program run by the U.S. Department of Com-

[1] Directive (EC) 95/46 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 [1995] OJ L281/31 (the ''Data Protection Directive'').

 ISSN 1538-3423

merce.[2] While Safe Harbor has proved to be a popular data transfer mechanism, the Safe Harbor Principles and other relevant documents agreed between the U.S. government and the European Commission do not directly address several important questions regarding Safe Harbor membership. One of the most vexing questions which often arises in practice is what implications Safe Harbor membership holds for a company that considers itself to be a ''data processor.''

I. The Concepts of Data Controller and Data Processor

EU data protection law distinguishes between the concepts of ''data controller'' and ''data processor.'' A data controller is a natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data, whereas a data processor is a natural or legal person which processes personal data solely on behalf of the data controller.[3] In practice, this means that a data controller has autonomy to determine how personal data are collected and processed, while a data processor is supposed to act only upon the direction of a data controller. However, there is intense discussion in Europe about where the borderline lies between the concepts of data controller and data processor.[4] In many cases, a company may act as a data controller with regard to certain functions of data processing and as a processor with regard to other functions, so that it can be difficult to distinguish the two sets of functions.

The importance of the distinction between a data controller and a data processor in the Safe Harbor context arises because of the obligations that are put on a company when it joins the Safe Harbor. Upon membership of the Safe Harbor, a company is in effect pledging to the world that it complies with the Safe Harbor Principles in processing personal data (called ''personal information'' in the Safe Harbor documents); if it does not so comply, then it may be liable under the U.S. Federal Trade Commission (FTC) Act.[5] Thus, the ability to comply with the Safe Harbor Principles is of critical importance so that the Safe Harbor member company may avoid legal liability.

The Safe Harbor documentation does not directly address the question of whether data processors are eligible for Safe Harbor membership, and the Safe Harbor Principles themselves do not use the terms ''data controller'' or ''data processor.'' The Safe Harbor decision of the European Commission and related documents refer instead to the concept of ''organization,'' which term sometimes seems to be used in a colloquial sense as any entity processing personal data (whether data controller or data processor)[6] and other times more specifically in the sense of ''data controller,''[7] and to the concept of ''agent,'' which seems to be used in the sense of data processor.[8]

Data processors are eligible for membership in the Safe Harbor, as the following considerations demonstrate:

- In view of the uncertainty under European data protection law regarding the distinction between a data controller and a data processor, restricting Safe Harbor membership to companies that are clearly data controllers would greatly restrict the number of companies that could join.

- The Safe Harbor Principles and supporting documentation do not indicate any intent of the United States or the EU to restrict Safe Harbor membership to data controllers. In fact, Safe Harbor FAQ 10 asks ''When data is transferred from the EU to the United States only for processing purposes, will a contract be required regardless of participation by the processor in the safe harbor?'', which clearly contemplates that data processors may join.

- The Department of Commerce ultimately approves the Safe Harbor applications of companies and enters them on the list of Safe Harbor members, and the Safe Harbor list includes a number of companies that describe themselves as data processors.[9] Moreover, the European Commission never seems to have objected to data processors joining the Safe Harbor. This indicates that, over the eight years that the Safe Harbor has been in existence, a kind of customary law has crystallized allowing data processors to join it. Moreover, the Safe Harbor application process itself does not require a company to state whether it is a data controller or a data processor, indicating that this distinction is not relevant in determining whether a company may join Safe Harbor.

It may be asked whether much importance should be granted to the distinction between data controller and data processor in the Safe Harbor context, since the Safe Harbor Principles state that any interpretation of

[2] Commission Decision (EC) 2000/520 of 26 July 2000 pursuant to Directive (EC) 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the U.S. Department of Commerce [2000] OJ L215/7.

[3] Data Protection Directive, Article 2(d)-(e).

[4] Regarding the issues involved, see ICC Summary of the Workshop on the Distinction between Data Controllers and Data Processors, available at http://www.iccwbo.org/policy/ebitt/id17704/index.html.

[5] See Safe Harbor Principles, stating ''Where in complying with the Principles, an organization relies in whole or in part on self-regulation, its failure to comply with such self-regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts.''

[6] See, e.g., the Safe Harbor Decision, Recital 5, providing that ''The adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if *organisations* comply with the Safe Harbor Privacy Principles for the protection of personal data transferred from a Member State to the United States and the Frequently Asked Questions providing guidance for the implementation of the Principles issued by the Government of the United States on 21.07.2000'' [emphasis added].

[7] E.g., providing access to personal data under the Access Principle, which provides that ''individuals must have access to personal information about them that an *organization* holds . . .'' [emphasis added]. See Article 12 of the Data Protection Directive, which provides that access is a right to be exercised against the data controller.

[8] E.g., in the Safe Harbor Choice Principle, footnote 1 of which refers to an agent as a third party that performs ''task(s) on behalf of and under the instructions of the organization.''

[9] For example, the Safe Harbor member companies Acxiom; Database Marketing Technologies, Inc.; Davis Direct WorldWide; Global DM Solutions, Inc.; and Phoenix Data Processing, LLC.

  PVLR ISSN 1538-3423

them is to be based on U.S. law,[10] which knows no such distinction. However, the better view is that, while the Safe Harbor itself is an instrument of U.S. law, it is informed by EU data protection concepts, and was drafted as a response to those concepts in order to provide a legal basis for data transfers to the United States. Thus, while the basis for interpretation of Safe Harbor should be U.S. law, such interpretation should be informed by relevant concepts of EU data protection law where appropriate. Interpretation of Safe Harbor thus involves a balancing act between U.S. and EU legal concepts in which both sets of concepts should be considered, but neither is given complete dominance over the other.

The Safe Harbor documentation does not directly address the question of whether data processors are eligible for Safe Harbor membership, and the Safe Harbor Principles do not use the terms ''data controller'' or ''data processor.''

The lack of clarity in the Safe Harbor documents regarding terms such as ''organization'' and ''agent'' can create doubt for a company that is seeking to join the Safe Harbor and is unsure whether it would be considered a data controller or a data processor. To give an example, the Safe Harbor Access Principle provides that ''individuals must have access to information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.'' A legal duty to provide access for data protection purposes generally does not exist under U.S. law, so it is difficult to use U.S. law to interpret this principle. Under EU data protection law, access should only be granted by a data controller, and not by a data processor, so that this Principle would seem to apply only to Safe Harbor members that are data controllers. However, a company joining Safe Harbor which considers itself a data processor would understandably be reluctant to conclude that the Principle is not applicable to it, since it may be liable under the FTC Act if it is wrong.

Safe Harbor FAQ 10 raises a question in this regard, since it seems to state that Safe Harbor member companies who are data processors do not need to comply with most of the Safe Harbor Principles, and in effect only need to comply with the requirement to have in place a data processing contract between the U.S. organization participating in the Safe Harbor and the data controller in the EU. However, it is risky for a Safe Harbor member company to rely on this language to avoid complying with the rest of the Safe Harbor Principles, for several reasons. As explained above, it can be difficult for a company to state with confidence that it is only a data processor, and not also a data controller. Thus, a company joining the Safe Harbor and not implementing the Safe Harbor Principles beyond the requirement to have a data processing agreement in place with a European data exporter will be taking the risk that in case of a dispute it would be found to be a data processor. Moreover, many Safe Harbor member companies that refer to themselves as data processors have implemented most if not all of the other Safe Harbor Principles. It has thus become best practice for data processors joining the Safe Harbor also to comply with the other Safe Harbor Principles as outlined below, notwithstanding FAQ 10. Such compliance should not prejudice the status of a Safe Harbor member company as a data processor.

II. Practicalities of Safe Harbor Membership for Data Processors

Joining Safe Harbor requires more thought for a company that considers itself a data processor than it does for a company that considers itself a data controller. This is because, first of all, the company will have to decide how it describes itself in the relevant Safe Harbor documents, and secondly, because the policies and procedures it adopts to implement the Safe Harbor Principles need to be tailored to its status as a data processor.

The company should carefully consider how it describes itself in its policies and procedures, in order not to contradict statements it may have made in other contexts. For example, if a company has notified data processing to the European data protection authorities (DPAs) covering the processing of data that will be transferred to the United States under Safe Harbor, it may be difficult to justify considering itself a data processor for Safe Harbor purposes, since notification to the DPA is something that is typically done by a data controller. It is possible for a company to be a data processor with regard to one type of processing and a data controller with regard to another type of processing, so that if the company believes strongly that it is only a data processor for certain types of data transfers and processing in the United States, it should clearly differentiate such processing in its Safe Harbor policies from any other types of processing for which it may be a data controller, in order to avoid confusion.

The data processor joining Safe Harbor should have a privacy policy which explains how it implements the Safe Harbor Principles in its data processing practices. In a typical situation involving a Safe Harbor registration by a data processor, the company may have no direct contact with the individuals or companies whose personal data are being processed, and it is the data controller who engages the data processor to process data on its behalf (often the client or subsidiary of the Safe Harbor member company) that has such relationships. In such a situation, the only way for the data processor to comply with the Safe Harbor Principles is to indicate in its Safe Harbor policy that it is cooperating with the original data controller to comply with the Principles. In some national data protection regimes, it is not uncommon for data controllers and data processors to cooperate so that the processor may in effect

[10] See Safe Harbor principles, stating ''US law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by Safe Harbor organisations, except where organisations have committed to cooperate with European Data Protection Authorities.''

outsource compliance with certain obligations of data protection law to the data controller. A number of Safe Harbor policies that have been accepted by the Department of Commerce provide for procedures under which the Safe Harbor member who is a data processor may structure its compliance obligations so that they are fulfilled by cooperating with the data controller.[11] Ideally these steps should be memorialized in an agreement between the data processor and data controller.

In drafting the policy, compliance with the Safe Harbor Principles should be explained in a positive sense rather than a negative sense. That is, rather than stating that the member company cannot comply with a certain Principle by itself because it is not a data controller and does not have a direct relationship with the individual whose data it is processing, the company should indicate how compliance is based on cooperation between the company and the original data controller. It is advisable to avoid using the terms ''data controller'' and ''data processor'' in the policy unless there is a specific reason to do so, in order to avoid introducing EU legal terms into the policy (in the formulations below, the Safe Harbor member company is referred to as an ''agent'').

The following explains how each of the Safe Harbor Principles may be complied with in a case involving a data processor that does not have a direct relationship with the data subjects whose personal data it is processing; for each Principle, language is proposed that a company could use in its Safe Harbor policy. It is important to remember that drafting a Safe Harbor privacy policy requires an investigation of the member company's data processing practices, to ensure that it can comply with the Safe Harbor Principles. Thus, this language is just exemplary, and must be tailored to a company's specific situation before being used.

Notice Principle: Data subjects have to be informed about the collection of data and the purposes of such collection, how to contact the Safe Harbor member organization to inquire or complain, the types of third parties to which it discloses data, and the choices and means to limit their use and disclosure. Here is possible language for the Safe Harbor policy:

> ''As an agent processing personal information under the direction of its customers, XYZ COMPANY has no direct relationship with the individuals whose personal data it processes. XYZ COMPANY works with its customers to help them provide notice of data processing to individuals, including information concerning (1) the purposes for which personal information is collected and used; (2) a contact person to whom enquiries or complaints may be directed; (3) the types of third parties to whom personal information is disclosed; and (4) the choices and means that individuals are offered for limiting use and disclosure of personal information.''

Choice Principle: Individuals must be provided with the possibility of opting out of disclosure of their personal data to a third party and of their use for purposes other than those for which they were collected. However, it is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures. Opt-in consent must be obtained for the processing of ''sensitive data'' (meaning personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual). The Safe Harbor member company must thus determine whether companies to which personal data will be disclosed are data controllers or data processors, in order to determine whether or not individuals should be given a chance to opt-out of such disclosure. The data processor should agree on a procedure with the original data controller whereby the controller informs the processor about the purposes for which the personal data were originally collected and whether any individual has opted-out of disclosure to any third parties, and the processor should implement the individual's choice in such cases. Here is possible language for the Safe Harbor policy:

> ''As an agent processing personal information under the direction of its customers, XYZ COMPANY has no direct relationship with the individuals whose personal data it processes. XYZ COMPANY may disclose personal data to third parties in the following instances: [INSERT DETAILS]. XYZ COMPANY works with its customers to help them inform individuals about the possibility of such disclosures and provide individuals with the choice of opting-out of them. XYZ COMPANY only processes personal information for purposes that are compatible with those for which it was originally collected or subsequently authorized by the individual. [Statement that XYZ COMPANY does or does not process any sensitive data, and an explanation of how opt-in consent is provided for the processing of any such data.]''

Onward transfer Principle: The Safe Harbor member company seeking to transfer personal data to another company or entity that has not subscribed to the Safe Harbor Principles must ensure that the Safe Harbor notice and choice Principles have been complied with regarding the onward transfer. However, if the third party is an agent, then the company must either ascertain that the third party subscribes to the Safe Harbor Principles or is subject to EU data protection law or another EU adequacy finding, or it must enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the Safe Harbor Principles. The Safe Harbor member company must thus determine whether companies to which personal data will be transferred are data controllers or data processors, to determine what steps should be taken. Here is possible language for the Safe Harbor policy:

> ''Personal information may be transferred to [insert information about data controllers] and [insert information about data processors]. Transfers to [insert information about data controllers] are covered by the provisions in this Policy regarding notice and choice. XYZ COMPANY has concluded agreements with [insert information about data processors] requiring that they provide at least the same level of privacy protection as do the Safe Harbor Principles.''

Any company processing personal data in the United States is subject to U.S. law, which includes an obliga-

[11] Examples include the Safe Harbor policies of the companies Global Village Marketing & Data Services, Inc. (available at http://www.globalvillagemktg.com/legal/safeharbor.php) and Global DM Solutions (available at http://www.globaldmsolutions.com/privacy.html#safe_harbor).

  PVLR ISSN 1538-3423

tion to cooperate with lawful requests for access to data by law enforcement authorities. It may thus be advisable for the company to include some language about the possibility of law enforcement access to personal data in its Safe Harbor policy. The Safe Harbor framework contains exceptions to adherence to the Principles for the purpose of meeting law enforcement requirements;[12] however, the scope of these exceptions, and their legal effect, is controversial. There are two possible strategies that can be followed here, namely either to rely on the exceptions in the Safe Harbor for law enforcement access to data (i.e., in effect to categorize law enforcement access as falling outside the Safe Harbor framework), or to explain the possibility of law enforcement access as a kind of onward transfer under the Safe Harbor framework. Possible language for the first approach (relying on the law enforcement exception in Safe Harbor) could be the following:

> ''As set out in the US Safe Harbor Principles, adherence to the Principles may be limited to the extent necessary to meet national security, public interest, or law enforcement requirements.''

Possible language for the second approach (explaining the possibility of law enforcement access as a kind of onward transfer under the Safe Harbor framework) could read as follows:

> ''Please be aware that in certain circumstances, it is possible that personal information may be subject to disclosure pursuant to judicial or other government subpoenas, warrants, or orders.''

Security Principle: A Safe Harbor member company must take reasonable precautions to protect data from loss, misuse and unauthorized access, disclosure, alteration and destruction. Transfers to the United States for the purpose of ''mere processing'' additionally require the EU-based controller and the U.S.-based processor to enter into a data processing agreement (an ''Article 17 contract'' under that article of the Data Protection Directive) to protect the controller's rights under EU law; such contracts must also be concluded between the U.S. data importer and any third parties to whom it outsources processing. Here is possible language for the Safe Harbor policy:

> ''XYZ COMPANY offers a high level of data security to protect message data from loss, misuse and unauthorized access, disclosure, alteration and destruction. As an agent processing personal information under the direction of its customers, XYZ COMPANY has concluded a contract with its customers specifying the conditions under which personal information received from the EU are processed and kept secure. XYZ COMPANY has appropriate contractual language in place with third party data processors providing that they must apply the Safe Harbor Principles to the processing of personal data received from XYZ COMPANY.''

Data integrity Principle: The personal data processed must be relevant for the purposes for which they are to be used. Furthermore, personal data may not be processed in a way that is incompatible with the purposes for which they have been collected or subsequently authorized by the data subject. Reasonable steps must be taken to ensure that data are reliable for their intended use, and that the data are accurate, complete, and current. Here is possible language for the Safe Harbor policy:

> ''XYZ COMPANY only processes personal data that are relevant to the services it provides, and only for purposes compatible with those for which the data were collected. As an agent processing personal information under the direction of its customers, XYZ COMPANY works with its customers so that they can provide a way for individuals to correct their data.''

Access Principle: Individuals must have access to all personal data processed by the Safe Harbor member company, and must be able to correct, amend or delete inaccurate data. The right of access is limited by the principle of reasonableness, and companies may charge a fee to provide access and can limit the number of access requests within a given period. Here is possible language for the Safe Harbor policy:

> ''As a data processor, XYZ COMPANY has no direct relationship with the individuals whose personal data it processes. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct his query to the client of XYZ COMPANY (the data controller) which has transferred such data to the XYZ COMPANY for processing. The client will then provide access to the individual as determined under the applicable local data protection law.''

Enforcement Principle: The Safe Harbor member company must provide recourse for individuals by joining a self-regulatory privacy program that includes an alternative dispute resolution mechanism, or by agreeing to cooperate with EU DPAs. The wording of a Safe Harbor policy with regard to enforcement need not be any different for a data processor joining Safe Harbor than it would be for a data controller.

III. Conclusions

Membership of Safe Harbor by a data processor gives rise to a number of issues, but these should not stop a company from joining the Safe Harbor. Safe Harbor membership by a data processor is wholly justified under the law and the documents that form the basis of Safe Harbor, and it should be possible for companies that are data processors to structure their policies and procedures to comply with the Safe Harbor Principles, while maintaining their status as data processors. Safe Harbor is thus a viable data transfer mechanism for data processors that process personal data exported to the United States from Europe.

[12] See the Safe Harbor Principles, which provide ''Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its noncompliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization. . . . Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis . . .''