

Data Transfers From The European Union: Compliance With The Safe Harbor

This memorandum summarizes the requirements for complying with the safe harbor for the transfer of personal data from European Union member states. These requirements apply to you *only if* you receive personal data from European Union member countries (or “states”), and they only cover the data that you receive from those states.

We begin the memorandum with a brief background to the safe harbor established by the Department of Commerce for complying with the privacy requirements imposed by the European Union member states. We then discuss when it is necessary to comply with the safe harbor, we explain the specific requirements that you must meet to comply with it, and outline the steps that we suggest be taken to ensure compliance. At the end of our discussion of each specific safe harbor requirement, we explain the difference, if any, between that requirement and the requirements imposed upon you under the Gramm-Leach-Bliley Act (GLBA).

I. Introduction

On October 24, 1995, the European Parliament and the Council of the European Union adopted a comprehensive Directive¹ concerning personal data.² This Directive establishes personal data privacy as being a fundamental right and freedom that Member States should protect.³ Thus, the processing of personal information must conform to the Directive.⁴ For example, personal information may only be collected for specified, explicit and legitimate purposes and cannot be processed in a way that is incompatible with those purposes.⁵

1 European Community Directive on Data Protection (“European Community Directive”), OJ No C ____, x.x.1995. Each EU member state is required to implement the Directive requirements through the enactment of regulation or statutes. The precise parameters of each state’s implementing provisions vary.

2 **Personal Data:** Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

3 European Community Directive, Article 1.

4 **Processing:** Any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination blocking, erasure or destruction.

5 European Community Directive, Article 6(1)(b).

II. When Is It Necessary to Comply with the Directive?

In assessing whether your compliance with the Directive is necessary, you must consider the circumstances under which your organization is receiving personal data from the European Union. For example, if your organization has a web site that collects personal data, then you may receive personal data from residents of the European Union. In that case, you must be in compliance with the Directive with respect to that data. You should keep in mind that, even if your compliance with the Directive is necessary, it is only necessary with respect to the personal data that you receive from the European Union (and not with respect to all data that you collect).

If you have any subsidiaries located in European Union member states, then they are automatically subject to the Directive (and already should be complying with it). Any information that you receive from them also is subject to the Directive. In that case, however, you may simply follow your subsidiaries' procedures for compliance. This approach would bring you into compliance with the Directive with relatively little additional effort on your part.

Once you have assessed how and when your organization receives personal data from the European Union, you can decide the best means for complying with the Directive. There are essentially three ways to comply:

- (1) **Direct compliance.** One method of compliance is direct compliance, meaning simply that you directly comply with the requirements of the Directive as implemented by the relevant European Union member state from which the data originates. In situations where an organization has a subsidiary that is located in an European Union member state that is already complying with the Directive (as mentioned in the example above), or where the organization's business is primarily based upon personal data transfers from the European Union, then direct compliance may be the optimum choice for compliance.
- (2) **Compliance by contract.** A second method of complying with the Directive is to enter into a contract with the specific party or parties from whom you are receiving the data, pursuant to which you promise to provide the requisite privacy protections. If your receipt of personal data from the European Union is likely to occur only once or very infrequently, the contract option is advisable. Likewise, if you will be receiving data only from one or two parties in the same European Union member state, then even if you receive such data on a periodic basis, the contract method for compliance may make the most sense for you.⁶

⁶ You should note that if the parties choose to contract for privacy protection, the contract will need to be in a form that has been approved by the European Union Member State.

- (3) **Safe Harbor compliance.** The third method of compliance is to adhere to the seven requirements adopted by the Department of Commerce as constituting the safe harbor. In situations where personal data transfers from the European Union occur frequently or are received from several parties located in several different European Union member states, compliance with the safe harbor is likely to be the best option.⁷ Compliance with the safe harbor assures that personal data transfers from *all fifteen* European Union member states are properly protected. It automatically satisfies the requirement that any member states may impose for prior approval of personal data transfers, thereby removing the administrative burden of having to seek such approval before each transfer, and it reduces the scope of any legal action that may be taken against you by European citizens.

Because compliance with the safe harbor is the method that most United States organizations will choose to comply with the Directive, the remainder of this memorandum explains how to meet the safe harbor requirements. Before we turn to specifics, a final note on enforcement is necessary.

If you fail to comply with the Directive, then you risk being prohibited from receiving any personal data transfers from the European Union. While that reason alone should be enough to compel compliance, you also should realize that, in addition to such injunctive relief, there are a number of U.S.-based remedies available to individuals whose personal data has been transferred in violation of the Directive. Private causes of action are available for damages for the breach of privacy under common law, and several federal statutes affecting the transfer of data, including the Electronic Communications Privacy Act of 1986, the Telecommunications Act of 1996, and the Fair Credit Reporting Act, allow individuals to recover damages and attorneys' fees for any violations. Additionally, the Federal Trade Commission has broad jurisdiction and the authority to bring actions for any failure to adhere to stated privacy practices.

III. The Safe Harbor

To avoid significantly hampering the exchange of personal data between the United States and the European Union, the Department of Commerce worked closely with the European Commission to develop a "safe harbor" framework that provides a streamlined means for United States companies to comply with the Directive. The safe harbor consists of **seven privacy principles** and requires organizations to self-certify compliance with those principles annually to the U.S. Department of Commerce. Compliance with the safe harbor can

⁷ For any U.S. organization receiving personal data from EU residents through an Internet website, safe harbor compliance is almost certainly the best option.

be accomplished either by choosing to join an industry self-regulatory program or by developing your own self-regulatory privacy policy. Most organizations who have participated in the safe harbor to date have chosen to develop their own privacy policy.

If you decide to participate in the safe harbor by implementing your own privacy policy and certifying your compliance with it to the Department of Commerce, you will need to adhere to ***seven affirmative privacy requirements***. These are discussed below. These requirements will apply only to the personal data that you receive from European Union member states – they do not impact your treatment of any other information or the obligations imposed on you with respect to such other information under the GLBA.

The seven safe harbor requirements are similar in many ways to the requirements imposed under the GLBA but, overall, they impose more exacting and detailed obligations. Some of the requirements will look familiar to you (such as the notice and choice requirements), some will seem familiar but are actually more complex (such as the focus on matching each piece of information with a purpose and use before collecting it), and others will be entirely new (such as the concept of verification). Following our discussion of each requirement below, we describe in general terms how each differs from the requirements imposed under the GLBA. That said, you should recognize that compliance with the European Union safe harbor requires considerable effort. Thus, you may want to consider developing a privacy policy that will apply only to European Union citizens and maintain a separate privacy policy for all others.

1. The Notice Requirement

Under the safe harbor notice requirement, individuals must be informed of the purposes for which their data is collected and used, how to contact the organization with inquiries and how they can limit the collection of data. Specifically, the safe harbor notice requirement requires that consumers be given notice of each of the following:

- The information that you collect about them
- The purposes for which the information is collected
- How the information is used
- How the consumer may contact the collector with complaints or inquiries
- With whom you share information about the consumer
- The options consumers have to limit the use and disclosure of their personal data

This information must be posted clearly and conspicuously and use language that is easy to understand.

In order to comply with the notice requirement, you will need to communicate with all of the divisions in your organization and obtain complete lists of what information is being collected, for what purpose, and whether and with whom it is being shared. Complying with this notice requirement also will assist your organization in reviewing any mechanisms it has in place for responding to customer complaints and for assessing whether those mechanisms are equipped to handle complaints related to personal data transfers.

The GLBA notice requirement is similar, but the specific disclosures required by the safe harbor are more comprehensive. Like the safe harbor, the GLBA obligates you to disclose the nonpublic personal information that you collect, the third parties to whom you may disclose such information, and the consumer's right to "opt-out" of certain information disclosure. The GLBA, however, does not require you to tell consumers how to file inquiries or complaints or require you to disclose all of the ways that the information you collect may be used. Only if you are taking advantage of the service provider/joint marketing exception does the GLBA require you to state how the information you collect will be used. In comparison, if you share information completely outside of a GLBA exception, you need only state the categories of information you may disclose and the categories of third parties to whom you may disclose it. You need not otherwise say how that information will be used. The requirement to communicate disclosures in clear and conspicuous language is the same under both the safe harbor and the GLBA.

2. The Choice Requirement

Under the safe harbor choice requirement, consumers must be provided with readily available and affordable mechanisms to direct an organization to not use or disclose information in at least two situations:

- **Third party sharing.** If the organization shares personal data with a third party, even if the sharing is for the same purpose for which the data was originally collected; and
- **Incompatible purposes.** If the collector may use the data for a purpose that is "incompatible" with the purpose for which it was originally collected.

Organizations must allow consumers to exercise this right – commonly referred to as an "opt out" right – at any time, subject to reasonable limits established by the organization. An organization may require sufficient information to confirm the identity of the individual requesting the "opt out," if the organization determines that such measures are prudent or desirable.

The opt-out requirement recognizes that in certain circumstances it may be impracticable to provide consumers with the opportunity to opt out *before* their personal data is

used. Thus, for purposes of an organization's direct marketing efforts, an organization may use personal data and give the opt-out notice *simultaneously*, thereby allowing the individual to decline (at no cost) to receive any further direct marketing communications.

In certain circumstances, the safe harbor choice requirement imposes an even more stringent obligation on organizations seeking to share personal data. If the data in question includes "sensitive information,"⁸ then the consumer must exercise *an affirmative choice* to allow that information to be shared with a third party or used for a purpose other than it was originally collected. In other words, for sensitive information, the organization must offer consumers the opportunity to "opt-in."⁹

In terms of complying with the choice requirement, the most important first step you can take is to ascertain whether you transfer any "sensitive information" to third parties or use any data for reasons other than the reason for which it is collected. Again, it will probably be necessary to contact every division in your organization, from the human resources department to the web site development office, in order to ensure you have covered all of your bases on this information. Your ultimate goal, of course, is to establish failsafe methods for individuals to exercise their opt-out or opt-in rights.

In comparison to the GLBA, the safe harbor choice requirement is much more restrictive than the GLBA opt-out. It covers a broader range of information and provides no exceptions under which information sharing is permitted and no opt-out is required. Thus, for example, the safe harbor choice requirement contains no exception for joint marketing – meaning that you must give consumers the right to opt-out of information sharing with third parties with whom you jointly market financial products. In contrast, under the GLBA, you may share information with third parties pursuant to a joint marketing agreement without first offering consumers the right to opt out of such information sharing.

3. The Onward Transfer Requirement

The transfer of information onward to third parties after it is received by an organization gives rise to a separate safe harbor requirement.

8 Sensitive information: 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.

9 The opt-in is *not required* in these limited circumstances:

- a) If the processing of the data is in the vital interests of the individual;
- b) If it is necessary for the establishment of legal claims or defenses;
- c) If it is required to provide medical care or diagnosis;
- d) If it is being processed by a non-profit organization and the individual is a member of the organization or has regular contact with the organization;
- e) If it is necessary to carry out the organization's obligations in the field of employment law; or
- f) If it is related to data that are manifestly made public by the individual.

Once you have provided consumers with the requisite notice about your organization's information practices and choice concerning their ability to preclude you from information sharing, you may transfer personal data to third parties. Those third parties must themselves then meet the notice and choice requirements. Ordinarily, you have no responsibility for their compliance. When the third party to whom you transfer data is acting as your agent, however, you are required to ensure that the third party also subscribes to the safe harbor principles. You can discharge your obligation either by determining that the third party is itself subject to the Directive, or by requiring the third party to enter into a written agreement to provide the same level of privacy protection as required by the safe harbor. Once you have assured the third party's compliance, the third party/agent need not provide notice and choice separately to consumers. Moreover, once you have assured compliance, you will not be held liable for the third party's misuse of the information, unless you knew or should have known of the misuse and did not take reasonable steps to stop it.

To provide your organization with the best protection, you should ensure that all of your employees understand the issues surrounding the onward transfer of personal information and that they have an easy way to report any suspected misuse.

In comparison to the GLBA, the safe harbor onward transfer requirement is more detailed and more complex. Under the GLBA, everyone who collects and shares nonpublic personal information is subject to the notice and opt-out requirements, including any third party with whom you share nonpublic personal information. Thus, unlike under the safe harbor, there is no need for you to determine whether third party compliance is required, and third party compliance is never excused. Similar to the safe harbor, under the GLBA you will not be held liable for a third party's misuse of information. Under the joint marketing exception, however, you are required to incorporate language in your joint marketing agreements prohibiting third parties from disclosing information other than for the purposes for which you have disclosed it.

4. The Data Security Requirement

The safe harbor data security requirement simply requires organizations to take reasonable steps to secure personal data, especially any sensitive information. Data is not secure if it is available to every employee in an organization. The areas of greatest concern are the loss, misuse, unauthorized access, inadvertent disclosure, alteration or destruction of personal data.

In order to meet this requirement, your current data storage systems should be evaluated for security against data loss and hacking. Most importantly, you must ensure that the systems protecting any sensitive data, are as secure as possible. Additionally, in order to provide the most secure environment for the personal data you collect and store, you

should consider maintaining a list of every employee or type of employee who has access to the different kind of personal data. To the extent possible, you should then reduce the list to only those employees who absolutely need access to such information.

The security requirement is essentially the same under the GLBA. While the GLBA requires you to disclose to your consumers your practices for protecting the confidentiality and security of the data you collect about them (such as the physical, electronic and procedural safeguards that you take to protect it), like the safe harbor security requirement, the GLBA does not require that you employ any particular security procedures.

5. The Data Integrity Requirement

The requirement consists of two separate directives. First, organizations must ensure that data collected for a specific purpose be limited to the type of information that is necessary for that purpose and that it not contain any extraneous information. For example, if a consumer purchases a television, the seller might legitimately need to know the consumer's name and credit card number (for the purchase) and the consumer's address (for tax purposes). For purposes of the television purchase, if the seller also collects information regarding whether the consumer purchased the same brand as his old television, the seller would violate the data integrity principle, because it would be collecting more information than necessary to complete the transaction. Second, the data integrity principle requires organizations to ensure, to the extent possible, that their data is reliable, accurate, complete and current for its intended use.

Compliance with the data integrity requirement is relatively onerous. It will require each division in your organization that collects personal data to determine the precise purposes for which each category or item of information collected. For example, your organization may determine that information such as a consumer's name, address, phone number and social security number is collected for two reasons: billing purposes and identification. Once the divisions have completed this analysis, it is advisable to maintain the list for reference in the case of consumer complaints or disputes.

The GLBA does not impose such an explicit data integrity requirement. Rather, as with respect to data security, the GLBA simply requires that you disclose to your consumers (in a general statement on your privacy form) your practices for protecting the integrity of the data that you collect about them (such as the physical, electronic and procedural safeguards that you take to protect it). The GLBA does not require that you employ any particular procedures to ensure data integrity, although certain specific GLBA requirements implicitly ensure that the information you collect is used only for the purposes for which you collected it. The joint marketing exception is one such example of this.

6. The Access Requirement

The safe harbor access requirement balances two competing principles. First, the access requirement dictates that, in some cases, individuals must have access to the personal data collected about them and be able to amend, correct or delete such information. The safe harbor recognizes, however, that providing such access may be extremely burdensome and expensive or otherwise impracticable for an organization to achieve. The access requirement thus requires organizations to balance the challenges of providing access with the individual's reasons for wanting access. For example, if the information is used for decisions that significantly affect the individual (such as getting a mortgage or being turned down for a job), then the organization must disclose the information, even if it is difficult or expensive to provide.

While an organization must make a good faith effort to provide access to information requested, the access principle *does not* create any affirmative obligation to retain, maintain, reorganize, or restructure personal information files. Additionally, the organization is permitted to charge a reasonable fee for access to the information.

In certain cases, an individual's request for access to information may be denied outright. For example, an organization can refuse to provide access when the disclosure would include "confidential commercial information,"¹⁰ or when it is likely to interfere with the public interest or national security. If personal information is processed *solely* for research or statistical purposes, access also may be denied. Several other specific situations exist,¹¹ but whenever an organization denies access, the organization carries the burden of demonstrating why the denial was appropriate.

In order to streamline the process for providing such access, you should review the types of personal data your organization collects and categorize the information according to its ease of accessibility and the projected importance of that information to your customers. To answer requests for personal data that falls into an excepted category, you

10 **Confidential commercial information:** As defined in the Federal Rules of Civil Procedure, information that an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. Organizations may deny or limit access to the extent that granting it would reveal its own marketing plans or classifications or would breach contracts or an obligation to keep information confidential that would normally be undertaken or imposed.

11 Other reasons for denying or limiting access are:

- a) Interference with execution or enforcement of the law;
- b) Interference with private causes of action;
- c) When disclosure of the information would include information belonging to someone else and could not be redacted;
- d) It would result in a breach of legal or other professional privilege or obligation;
- e) It would result in a breach of on-going sensitive business negotiations; or
- f) It would prejudice employee security or grievance proceedings.

should develop written policies explaining why access to certain information cannot be granted. If there are costs associated with providing access to certain kinds of personal data, you should determine in advance of any requests a reasonable cost to charge for such access.

The GLBA does not have a requirement comparable to the access requirement.

7. The Enforcement Requirement

Enforcement is the cornerstone of the safe harbor framework, because it ensures compliance with the safe harbor. Additionally, it provides recourse for individuals whose personal data is used or transferred inappropriately and provides private consequences for organizations that fail to comply. According to the safe harbor enforcement requirement, effective privacy protection must include a means for verifying that an organization is complying with the safe harbor privacy principles, a means for resolving disputes, and a means for providing a remedy. In order to accomplish these goals, the safe harbor mandates that consumers have the option of relying on an independent third party for dispute resolution, as discussed in more detail below.

As compared to the GLBA, the safe harbor adds another level of enforcement. Under the GLBA, only the regulatory body with regulatory jurisdiction over the financial institution in question (for example, the fifty states for insurance providers and the federal banking regulators for banks) has the authority to enforce the GLBA requirements, which it may do in an administrative proceeding. In contrast, the safe harbor authorizes private rights of action against organizations for failure to comply. Moreover, unlike the GLBA, it permits sanctions to be imposed on noncomplying organizations and permits the recovery of damages by consumers able to demonstrate harm.

Verification

An organization may verify its compliance with the safe harbor either through self-assessment (which takes the form of a signed certification from a corporate officer or other authorized representative at least once a year) or through an outside compliance review (which takes the form of a signed certification from the outside reviewer or by the corporate officer at least once a year). Pursuant to either method, an organization must first have distilled into a privacy policy any information necessary to demonstrate its compliance with the notice, choice, onward transfer, security, data integrity and access requirements. Once that privacy policy is in place, the verification process can move forward.

The self-assessment method requires the organization to do the following:

- (1) Show that its published privacy policy regarding personal data received from the European Union is:
 - accurate;
 - comprehensive;
 - prominently displayed;
 - completely implemented; and
 - accessible.
- (2) State that the privacy policy conforms to the safe harbor principles.
- (3) Establish and notify consumers of its complaint mechanisms and dispute resolution process.
- (4) Train its employees about the implementation of the privacy policy and discipline them for failure to follow it.
- (5) Establish internal procedures for periodically conducting objective review of compliance with the above.

The outside compliance review method requires the organization to do the following:

- (1) Choose a respectable and established reviewer.
- (2) Demonstrate that its privacy policy regarding personal data received from the European Union complies with safe harbor principles and that its policy is being complied with.
- (3) Demonstrate that consumers are informed of the complaint mechanisms.

Dispute Resolution and Remedy

As mentioned above, to comply with the safe harbor enforcement requirement, an organization must implement a mechanism for resolving consumer disputes or complaints and provide a means for remedying the problem. In order to accomplish these goals, the safe harbor mandates that consumers have the option of relying on an independent third party for dispute resolution (“independent dispute resolution mechanism”). This independent dispute resolution mechanism must be an independent third party able to resolve complaints in an orderly fashion.

Organizations have three options from which to select an independent dispute resolution mechanism. First, an organization may choose to use a third-party dispute mecha-

nism offered by organizations such as BBBOnline, TRUSTe, AICPA, WebTrust or the Direct Marketing Association. Second, the organization may choose an outside arbitration and mediation service that hears complaints. Third, the organization may choose to cooperate with the “European Union Data Protection Authorities.”¹²

Regardless of the mechanism chosen, it should be independent, readily available, and affordable for individuals to use to resolve their complaints or disputes. The dispute resolution mechanism may award damages to consumers who can show that they were harmed and may levy sanctions on organizations that fail to remedy a particular problem or persistently fail to remedy problems. The dispute resolution mechanism also may report compliance failures to appropriate governmental bodies, such as the Federal Trade Commission or the Department of Commerce.

IV. Qualifying for the Safe Harbor

Once an organization’s privacy policy has been developed and implemented, its efficacy has been verified, and an independent dispute resolution mechanism has been chosen and established, the organization can begin the process of self-certifying its compliance with the safe harbor to the Department of Commerce. Self-certification can be accomplished by filing a letter containing the information outlined below. The letter must be signed by a corporate designee and formally filed with the Commerce Department. The Commerce Department will evaluate the letter and, upon approval, post the names of all organizations who have certified compliance with the safe harbor. This certification process must be completed annually.

At the very least, the following information should be included in your self-certification letter:

- (1) The name of the organization, mailing address, email address, telephone and fax numbers;
- (2) A description of the activities of the organization with respect to personal information received from the EU; and
- (3) A description of the organization’s privacy policy for such personal information that includes the following:
 - Where the privacy policy is available for viewing by the public;

¹² **European Union Data Protection Authorities (DPAs).** European Union level panels who have the power to: (a) investigate data processing activities and monitor application of the Directive; and (b) intervene in the processing by ordering blocking, erasure, or destruction of data as well as by banning its processing.

- Its effective date of implementation;
- Contact information for the handling of complaints, access requests, and any other issues arising under the safe harbor;
- The specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (i.e., the Federal Trade Commission or the Department of Transportation);
- The name of any privacy programs in which the organization is a member;
- The method of verification (self-assessment or outside review);
- The Independent Recourse Mechanism;
- European Union countries that you receive information from;
- The organization's industry sector (available from the Department of Commerce web site, an example is "INS" for insurance);
- Amount of organization sales (this information is not posted by the Department of Commerce); and
- Number of employees (this information is not posted by the Department of Commerce).