BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

In today's business world, data typically are not transferred once and then locked away, but are often re-exported to third parties. The Safe Harbor framework contains rules for such ''onward transfers,'' but they do not provide full answers to many questions. The onward transfer principle is one of the most significant components of the Safe Harbor framework, and its importance has increased markedly as onward transfers of personal data have become the rule rather than the exception.

A number of uncertainties about the onward transfer principle and its application, and differing views in the European Union and the United States about the effect and scope of the principle, can carry risks for Safe Harbor member companies. While these risks cannot be totally eliminated, the author offers a number of steps that can be taken to reduce them to an acceptable level.

Onward Transfers of Personal Data Under the U.S. Safe Harbor Framework

BY CHRISTOPHER KUNER

Christopher Kuner, a partner with Hunton & Williams LLP, Brussels, ckuner@hunton.com.
The author is grateful to the Oxford Internet Institute of Oxford University, where this article was completed during a stay as a Visiting Fellow in the summer of 2009. Thanks are also due to Cédric Burton, Jörg Hladjk, and Olivier Proust for their valuable input.

Mr. Kuner received a 2010 Burton Award for Legal Achievement, for this article.

I. Introduction

The Safe Harbor framework has proven to be one of the most popular and effective ways to provide an adequate level of data protection for the transfer of personal data to the United States. Under the European Union Data Protection Directive,[1] the United States

[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.

 ISSN 1538-3423

does not offer an ''adequate level of data protection,'' which results in a prohibition against data transfers from the EU, unless a viable legal mechanism for the transfer is implemented. Since enactment of the European Commission adequacy decision covering the Safe Harbor,[2] over 1,800[3] U.S.-based entities have joined the Safe Harbor system, and its use has contributed to enhanced awareness of European data protection requirements by U.S. entities. On Dec. 12, 2008, an agreement was also announced between the U.S. Department of Commerce and the Swiss Federal Data Protection and Information Commissioner, extending the Safe Harbor to cover transfers of personal data from Switzerland (which is not an EU Member State) to the United States as well.[4] At the same time, the Safe Harbor was originally concluded in a climate of political tension, and many questions of interpretation were left unresolved. This leaves companies seeking to join and implement the Safe Harbor in the difficult position of having to make important interpretative judgments about it without the benefit of authoritative guidance.

In today's business world, data typically are not transferred once and then locked away, but are often re-exported to third parties. A typical example of such a re-export (referred to in EU data protection parlance as an ''onward transfer'') is when European employee data are transferred to a global human resources database in the United States, and are then made accessible to all employees worldwide via the Internet. In this situation, access to the database by the employees, and by any other parties (such as service providers who log in to it remotely in order to perform maintenance), is considered to be an ''onward transfer'' from the United States to those parties. If the service provider then subcontracts the maintenance of the database to other companies to provide around-the-clock services, there may be a long string of onward transfers, and it can become difficult to determine which third party has had access to the database, at what time, and for what purposes. The number of such onward transfers has increased drastically in the years since the Safe Harbor framework was finalized, particularly because of the rise in the outsourcing of data processing.

The Safe Harbor framework contains rules for onward transfers, but they do not provide full answers to many questions that arise for companies that transfer data from Europe, for Safe Harbor members in the United States that perform onward transfers, and for regulators who are called upon to assess the legality of such transfers. However, by examining in detail the Safe Harbor onward transfer principle and its underlying policies, it is possible to implement a series of measures that can reduce the legal uncertainty of transferring personal data based on the Safe Harbor onward transfer principle.

II. Rules for conducting onward transfers

A. Transfers to data controllers

The Safe Harbor onward transfer principle provides as follows:

> ''To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote[1], it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters 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 relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.''[5]

Endnote 1 to the onward transfer principle provides: ''It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.'' It should be noted that the principle also covers onward transfers to entities in the same corporate family.

Thus, onward transfers from a Safe Harbor member company in the United States to a data controller[6] may only be carried out if the Safe Harbor notice[7] and choice[8] principles are applied. This means that the indi-

---

[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] As of June 11, 2009, the number stood at 1,829.

[4] The relevant documents are available at http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=en and http://www.export.gov/safeharbor/swiss/eg_main_018498.asp. As the Safe Harbor principles applicable to data transfers from Switzerland are virtually identical to those applicable to data transfers from the EU, this article applies to onward transfers under both the EU and Swiss Safe Harbor frameworks.

[5] See Safe Harbor principles, available at: http://www.export.gov/safeharbor/eg_main_018247.asp.

[6] See section III below regarding the distinction between data controllers and data processors.

[7] The Safe Harbor notice principle reads as follows: ''An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party[1]''. Endnote 1 provides: ''It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures''.

[8] The Safe Harbor choice principle reads as follows: ''An organization must offer individuals the opportunity to choose

   ISSN 1538-3423

vidual whose data are subject to the onward transfer must have been given notice of the transfer and have had the opportunity to opt out of it. In many cases it will be impossible for the Safe Harbor member company itself to give notice to individuals and give them the chance to opt out of any onward transfers. Therefore, the Safe Harbor member should obtain contractual commitments from the parties that exported the data from Europe that appropriate notice has been given and the opportunity to opt out has been provided.

As the legal risks of data breaches or misuse of data by third parties have grown since the Safe Harbor framework was originally enacted, it is highly recommended that an agreement be signed between the original data importer and the third party receiving the data from it, even though the onward transfer principle does not explicitly require this. Such an agreement should bind the third party to process the data in accordance with the instructions provided to it and the Safe Harbor principles, and should also incorporate protections for the original data importer.

B. Transfers to data processors

Onward transfers to data processors may be carried out if one of the following applies:

> (1) *the third party ''subscribes to the Principles''*: This obviously covers cases in which the third party has formally joined the Safe Harbor, but it is at least arguable that it would also be sufficient if the third party accepted the Safe Harbor principles in a legally-binding fashion as the basis for its data processing (for instance, by incorporating them in its binding privacy policy), without formally joining the Safe Harbor.
>
> (2) *the third party ''is subject to the Directive or another adequacy finding''*: This allows for onward transfers to third parties located in the EU, or in a country that has been subject to a formal adequacy finding of the European Commission.[9]
>
> (3) *the transferor ''enters 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 relevant Principles''*: While no form for such an onward transfer agreement has been officially approved, unofficial templates do exist.[10]

C. Exceptions

Two of the Safe Harbor ''Frequently Asked Questions'' (FAQs)[11] limit application of the onward transfer principle in certain situations:

> ''FAQ 14—Pharmaceutical and Medical Products
>
> Does a pharmaceutical or medical device firm have to apply the Safe Harbor Principles with respect to notice, choice, onward transfer, and access in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices (e.g., a pacemaker)?
>
> No, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers, to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.''
>
> ''FAQ 15—Public Record and Publicly Available Information
>
> It is not necessary to apply the Notice, Choice or Onward Transfer Principles to public record information, as long as it is not combined with non-public record information and as long as any conditions for consultation established by the relevant jurisdiction are respected.
>
> Also, it is generally not necessary to apply the Notice, Choice or Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.
>
> Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the Safe Harbor.''

These exemptions are interpreted narrowly by European data protection authorities (DPAs), so Safe Harbor member companies are well-advised to limit their reliance on them.

(opt out) whether their personal information is (a) to be disclosed to a third party[1] or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice. For sensitive information (i.e. 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), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.'' Endnote 1 is the same as the endnote in the notice principle quoted above.

[9] At the time this article was finalized, such adequacy decisions covered Argentina; Canadian organizations subject to the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act); the Bailiwick of Guernsey; the Bailiwick of Jersey; the Isle of Man; Switzerland; the U.S. Safe Harbor system; and transfers of airline passenger data to the U.S. Department of Homeland Security (DHS). See http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

[10] For such a template, see Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edition Oxford University Press 2007) Appendix 9.

[11] Available at http://www.export.gov/safeharbor/eg_main_018237.asp.

III. Problems in practice

A. Distinguishing onward transfers to data controllers from those to data processors

The Safe Harbor framework contains different rules for onward transfers made to ''data controllers'' and those made to ''data processors.'' 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.[12] 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 (examples of a company acting as a data processor would include an IT maintenance company accessing a database to perform virus checking, and companies that provide a mere conduit for data flows as with telecom service providers and ISPs). There is intense debate in Europe concerning the difference between data controllers and data processors, and it can be difficult to distinguish between the two concepts.[13]

The distinction is made more confusing by the fact that the Safe Harbor decision of the European Commission and related documents (including the onward transfer principle) do not use the terms ''data controller'' and ''data processor.'' Instead, the Safe Harbor principles refer to an ''organization,'' which term sometimes seems to be used in a colloquial sense as any entity processing personal data (whether data controller or data processor),[14] and other times more specifically in the sense of ''data controller''[15], and to the concept of ''agent'', which seems to be used in the sense of ''data processor.''[16] The first sentence of the onward transfer principle refers to disclosures of information ''to a third party,'' but since EU regulators generally assume that parties to whom personal data are transferred are data controllers unless the opposite can be definitely proven, this should be understood to refer to a data controller.

When determining whether the party to which the Safe Harbor member company transfers data is a data controller or a data processor, it is safest for the Safe Harbor member company to assume that the third party is a controller, unless a watertight case can be made that it is only a processor. If it seems that the onward transferee may be both a controller and a processor, then it may also be possible to separate out the different tasks a company is performing, and apply the rules for onward transfers to data controllers in situations where the company seems to be a controller, and those for transfers to data processors in the remaining situations, though this distinction may be difficult to implement in practice.

B. Using the United States as a hub for global data transfers

Some companies join Safe Harbor with the aim of centralizing their international data transfers via the United States. That is, the parent company (typically U.S.-based) implements an IT architecture by which data processed by various company entities in the EU are transferred to the United States, where they are stored and made available for access by all company entities worldwide. In effect, this centralizes data access in the United States, and can result in considerable efficiencies in cost and employee productivity. However, this arrangement may be legally uncertain in some Member States.

Under European data protection law, a distinction is to be made between legal requirements that apply to the processing of data inside the EU Member States, and the requirements for establishing an adequate level of data protection for transfers outside the EU. As the Safe Harbor documents make clear,[17] the Safe Harbor only addresses the second set of requirements, i.e., those relating to the establishment of an adequate level of data protection for transfers outside the EU, but does not affect obligations regarding the processing of data in the Member States. Differences in the understanding of this distinction can be the cause of difficulties for companies conducting international data transfers.

The view among U.S. companies and the U.S. government is that onward transfers from Safe Harbor member companies should be governed solely by the Safe Harbor principles, given that the Safe Harbor principles state that any interpretation of them is to be based on US law.[18] However, some European DPAs take the position that onward transfers from Safe Harbor member companies must still have a legal basis under the applicable national law of the EU Member State from which they were originally transferred; the European Commission has also indicated that onward transfers under Safe Harbor must fulfill the basic requirements of European data protection law (such as the principle of proportionality).[19] This is because the DPAs consider Safe Harbor to be a mechanism providing an adequate

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

[13] See Christopher Kuner, ''Membership in the U.S. Safe Harbor Program by Data Processors'' BNA's *Privacy & Security Law Report*, Vol. 8, No. 19 (May 12, 2008) (7 PVLR 723, 5/12/08).

[14] 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].

[15] E.g., the access principle provides that ''individuals must have access to personal information about them that an *organization* holds. . .'' [emphasis added]. Under Article 12 of the EU Data Protection Directive, access is a right to be exercised against the data controller.

[16] E.g., in the Safe Harbor choice principle, endnote 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.''

[17] See Safe Harbor privacy principles, http://www.export.gov/safeharbor/eu/eg_main_018475.asp, stating that ''The Principles cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States.''

[18] 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.''

[19] See Non-Paper presented by the Commission, Meeting of the Council, 25 June 2007 (unpublished), p. 3, in which the Commission stated that any onward transfers by SWIFT under

  PVLR ISSN 1538-3423

level of protection for data transfers to the United States,[20] but not a mechanism to transfer data globally. In their view, using the onward transfer principle as a mechanism to transfer data globally reduces the level of protection afforded by EU law and therefore circumvents the application of Articles 25 and 26 of the EU Data Protection Directive.[21] In practice, this means, for example, that if data are transferred from the EU to a Safe Harbor member company in the United States, and the U.S. company then wants to perform an onward transfer of the data to another company (whether inside or outside the United States), a legal basis for the onward transfer would have to be found under the law of the EU Member State from which the data were originally transferred.

This position of the DPAs can have a devastating effect on the ability of the Safe Harbor member company to conduct onward transfers, since in many cases it will be difficult or impossible to find an applicable legal basis for onward transfers under the national law of the Member State from which the data were originally transferred to the United States. Problems can arise in particular in situations where the company transferring the data must notify its processing to the national DPA, which may include a requirement to list any onward transfers; at this point, the DPA may ask what legal basis will be used to justify the onward transfer, which can result in the data transfer outside of the EU being questioned.[22]

The divergent positions of the EU and the United States are both understandable from their respective points of view. However, the Safe Harbor does have detailed rules under which onward transfers may be conducted, which would seem to make the further application of EU law unnecessary once the data have left the EU. Indeed, one could ask what the purpose of the onward transfer principle would be if onward transfers under Safe Harbor would still have to comply with all details of EU Member State law.

Resolution of this dispute would require a political agreement between the EU and the United States, which is unlikely in the foreseeable future. However, companies conducting onward transfers can take the following steps to reduce the risk that they would be found in violation of European data protection law regarding onward transfers under Safe Harbor:

- The company should determine the position of the DPA(s) of the Member State(s) from which personal data are to be transferred to the United States under the Safe Harbor, and in particular whether a legal basis for onward transfers under national law is required.
- If the DPA does impose such a requirement, then the company needs to determine whether a legal basis for the onward transfer can be found under national law. Of course, the company could take the position that national law no longer applies once the data have been transferred to the United States, and that the onward transfers should be considered solely under the Safe Harbor principles. However, this position risks putting the company in conflict with the DPA, for example if the onward transfers have to be notified to the DPA in the course of the company filing notice of the transfer to the United States.
- The use of an ''assurance agreement'' (see below) can help assuage concerns that DPAs, works councils, or labor unions may have about the onward transfers.

Even in cases where the company decides to follow the ''U.S. approach'' and assess the legality of onward transfers solely under the Safe Harbor standard, it makes sense from a risk management point of view to implement strict controls on onward transfers. Uncontrolled onward transfers pose the risk of liability under both European and U.S. law (for example, under security breach notification requirements). Thus, it is advisable to implement both internal controls and contractual protections with third parties, covering issues such as the following:

- any parties to whom personal data are transferred should be obligated to observe strict data security requirements;
- the use of personal data for marketing purposes should be restricted; and
- parties to whom data are transferred should be required to obtain the consent of the Safe Harbor member company before engaging any subprocessors to process the data.

C. Lawful access to data as an onward transfer

The processing of personal data in the United States is obviously subject to U.S. legal requirements such as requests for access to the data from law enforcement authorities, producing evidence in litigation, and complying with administrative subpoenas. Such access raises questions under the Safe Harbor onward transfer principle.

Deviations from the Safe Harbor principles are allowed for the purpose of meeting lawful access requirements,[23] but the scope of these exemptions, and their legal effect, are controversial. While the language

---

the Safe Harbor must be in accordance with the principle of proportionality under EU law.

[20] See the Safe Harbor principles, http://www.export.gov/safeharbor/eu/eg_main_018475.asp, stating that the Safe Harbor was solely designed for the specific purpose of satisfying the Directive's adequacy standard.

[21] See, e.g., the guidelines of the French Data Protection Authority (CNIL) on international data transfers, ''Guide sur les transferts de données à caractère personnel vers les pays non membres de l'Union européenne,'' June 2008, http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/Guide-tranfertdedonnees.pdf, pp. 7 and 16.

[22] For example, in France, where it is generally required to file a specific annex on data transfers which need to be approved by the CNIL, which must include a listing of all recipients of the data. In Belgium as well, the notification form requires a list of all the countries of destination, together with a legal basis for the transfers.

[23] 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. . .''

seems directed mostly toward law enforcement access, the reference to ''statute, governmental regulation, or case law that create conflicting obligations'' could apply to almost any situation where U.S. legal requirements conflict with the requirements of the Safe Harbor. However, it would obviously defeat the purpose of the Safe Harbor if a blanket exemption from it applied to cases involving even minor conflicts with U.S. law. Thus, the purpose of the Safe Harbor would seem to require that the exemption be construed narrowly, and applied only in case of serious conflict with U.S. legal requirements.

In the United States, companies often interpret the lawful access exemption broadly, and in effect categorize lawful access as a kind of onward transfer under the Safe Harbor framework which is legalized under the exemption. In the EU, the DPAs generally categorize lawful access as falling outside the Safe Harbor framework entirely, so that, in their view, the exemption does not legalize onward transfers from Safe Harbor member companies.[24] This difference of opinion indicates the danger of relying too heavily on the lawful access exemption, and the wisdom of reserving its use for truly serious conflicts between the Safe Harbor principles and U.S. legal requirements. It is also advisable for the company to include some language about the possibility of law enforcement access to personal data in its Safe Harbor policy.[25]

IV. Compliance strategies

A. Internal steps

In order to minimize the chance of conflict, company management should adopt guidelines on the filing of notifications with the DPAs in Europe, or counsel should be involved to handle the notification process. In addition, it is important for everyone in the company to adopt the same strategy for communicating the company's approach regarding onward transfers, in order to demonstrate that the approach is not designed to evade the requirements of European law. Such strategy should include a detailed exposition of the steps that will be taken to protect the data in case of onward transfers (e.g., requiring third parties to subscribe to the Safe Harbor principles or to enter into written data transfer agreements).

B. Use of an ''assurance agreement''

Beyond the purely legal hurdles to conducting onward transfers, a number of non-legal issues may arise as well. For example, unions, works councils, and employees may raise objections if a Safe Harbor member company seeks to centralize the processing of employee data in the United States by having the data of its European employees transferred to the United States and then made available to various company entities worldwide based on the onward transfer principle.

One way of dealing with such concerns is by implementing an ''assurance agreement.'' This is a framework agreement that is signed by the U.S. parent company on the one hand, and the company's non-European affiliates on the other hand, and provides additional protection for the data beyond that provided by Safe Harbor membership. Such an agreement is not legally required under the Safe Harbor framework, but may help provide an additional comfort level for DPAs, works councils, and others who have concerns about widespread onward transfers by the company. An assurance agreement contains provisions that supplement the Safe Harbor principles, in order to demonstrate that the Safe Harbor member company takes its responsibility towards the European entities seriously and is willing to enhance its compliance level with regard to any onward transfers to non-EU entities. The following are some provisions which may be included in an assurance agreement:

- A commitment by the Safe Harbor member company to require any subsidiary located outside the EU to apply the Safe Harbor principles to any European data which the company makes accessible or transfers to such subsidiary.
- Attaching as annexes separate template onward transfer agreements (one for onward transfers to data controllers, and another for onward transfers to data processors, with the provisions of the templates adjusted accordingly), which the Safe Harbor member company will require subsidiaries to enter into in order to bind them to provide the protections contained in the Safe Harbor principles.
- In case of any controversy or dispute concerning the processing of European data by a subsidiary located outside the EU, a commitment by the Safe Harbor member company to facilitate communication between such non-EU subsidiary and the European subsidiary from which the data were originally transferred, and to use its best efforts to help the subsidiaries find a solution.

While the use of an assurance agreement is untested, and it may not be sufficient to allay concerns about onward transfers in all cases, it can be a helpful tool to demonstrate the willingness of the Safe Harbor member company to go beyond the minimum that is legally required and provide additional protection for onward transfers.

V. Conclusions

The onward transfer principle is one of the most significant components of the Safe Harbor framework, and its importance has increased markedly as onward transfers of personal data have become the rule rather than the exception. A number of uncertainties about the onward transfer principle and its application, and differing views in the EU and the United States about the effect and scope of the principle, can carry risks for Safe Harbor member companies. While these risks cannot be totally eliminated, a number of steps can be taken to reduce them to an acceptable level.

---

[24] See, e.g., the decision of the Belgian Privacy Commission in the SWIFT case (Belgian Privacy Commission, Decision of 9 December 2008, unofficial translation available at http://www.privacycommission.be/en/static/pdf/cbpl-documents/a10268302-v1-0-151208_translation_recommswift_fina.pdf, para. 123), stating at para 220 (p. 66) that Safe Harbor does not cover the disclosure by SWIFT of data to the U.S. Treasury to comply with lawful subpoenas.

[25] See the proposed language in *Kuner* (n 13).

  PVLR ISSN 1538-3423