



# ELECTRONIC COMMERCE & LAW



VOL. 15, NO. 25

**REPORT**

JUNE 23, 2010

## **U.S.-EU SAFE HARBOR**

The Düsseldorf Circle, an informal group composed of the 16 German federal state data protection authorities, recently issued a resolution explaining that companies in Germany sending/exporting Personal Data to U.S. companies cannot merely rely on the statement of the U.S. data importer claiming that it has a Safe-Harbor certification, but must conduct certain due diligence to determine if the U.S. data importer is in compliance with the U.S.-EU Safe Harbor Framework. Failure to follow the clarified due diligence practices contained in the Resolution could potentially lead to an enforcement action by German data protection authorities as well as reputation damage from unwanted media attention.

### **German Authorities Issue Privacy Decision Clarifying Due Diligence That Must Be Conducted on Companies Using The Safe Harbor Framework to Transfer Personal Data to the United States**

BY ROLF HÜNERMANN, MARC J. LEDERER, JOCHEN RIECHWALD, AND DR. CHRISTIAN ROLF, AND FRANCIS M. BUONO

*Rolf Hünermann and Dr. Christian Rolf are partners, and Jochen Riechwald is an associate, in the Frankfurt office of Willkie Farr & Gallagher. Francis M. Buono is a partner in the firm's Washington, D.C., office, and Marc J. Lederer is an attorney in the firm's New York office.*

**G**erman data protection authorities rendered a decision (the "Resolution")<sup>1</sup> at a meeting of the Düsseldorf Circle<sup>2</sup> on April 28-29, 2010, clarifying certain due diligence responsibilities for German compa-

<sup>1</sup> Sitzung des Düsseldorfer Kreises am 28./29. April 2010 in Hannover.

<sup>2</sup> The Düsseldorfer Kreis or Düsseldorf Circle is an informal working group composed of the 16 German federal state data protection authorities. Its decisions are not legally binding but they are of vital importance as they indicate the administrative practice of German data protection authorities.

nies that send/export personal data (“Personal Data”)<sup>3</sup> to U.S. companies that self-certify to the U.S.-EU Safe Harbor Framework (the “Safe Harbor”).

## Background on Cross-Border Transfers

Under the European Commission Data Protection Directive 95/46 (the “Directive”) of the European Union (the “EU”), cross-border information transfers of Personal Data are restricted by companies operating within the European Economic Area (the “EEA”)<sup>4</sup>.

Those companies operating within the EEA that wish to transfer/export Personal Data outside of the EEA, may do so if the company receiving/importing that Personal Data is located within a country that is deemed to have an “adequate level of data protection” by the European Commission. However, the United States has been adjudged by the European Commission not to have an adequate level of protection. Therefore, companies located in the EEA that wish to transfer (or provide remote access to) Personal Data to companies located within the United States, must use one or more of several approved methods for such Personal Data transfer. One of the more popular methods for such transfers is through the Safe Harbor.

## The Safe Harbor Framework

The Safe Harbor was approved by the EU in 2000. For a U.S. company<sup>5</sup> to join the Safe Harbor, it must go through a self-certification process, whereby the company certifies to the U.S. Department of Commerce that it is in compliance with the Safe Harbor, which consists of seven principles (the “Principles”): Notice<sup>6</sup>, Choice, Access, Transfer to Third Parties, Security, Data Integrity and Enforcement. Unless a company’s self-certification is rejected after review, it will be placed on the Safe Harbor list, which is made publicly available on a website managed by the U.S. Department of Commerce’s International Trade Administration.<sup>7</sup> Annual recertification is required for a company to be listed as “current” on the Safe Harbor list. Currently there are approximately 2,192 companies included on the Safe Harbor list, although a number of them are listed as being “not current.”

<sup>3</sup> Under EU Directive 95/46/EC—The Data Protection Directive, Chapter 1, Article 2(a) “personal data” means any information relating to an identified or identifiable natural person (“data subject”); 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.

<sup>4</sup> The European Economic Area comprises 30 members—the 27 EU countries plus Iceland, Liechtenstein, and Norway.

<sup>5</sup> Only U.S. companies that are subject to the jurisdiction of the Federal Trade Commission (the “FTC”), or the Department of Transportation with respect to air carriers and ticket agents, may participate in the Safe Harbor.

<sup>6</sup> Companies must notify individuals about the purposes for which they collect and use information about them through a privacy notice. These notices must provide information about how individuals can 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 for limiting its use and disclosure.

<sup>7</sup> <https://www.export.gov/safehrbr/list.aspx>.

## The Düsseldorf Circle Resolution

Concerned with the enforcement and control processes involved with self-certification under the Safe Harbor, the German data protection authorities stated that companies in Germany sending/exporting Personal Data to U.S. companies cannot merely rely on the statement of the U.S. data importer claiming that it has a Safe-Harbor certification, but must conduct certain due diligence to determine if the U.S. data importer is in compliance with the Safe Harbor Principles.

According to the Resolution, one item of due diligence that German data exporters must perform is to verify that the U.S. data importer has in fact made a self-certification to the Safe Harbor, as well as checking the certification date. The Resolution states that if the certification date is more than seven years old, then it is no longer valid. However, it is unclear how this “seven year rule” applies, since “valid” is not a term used in the Safe Harbor. A company’s compliance with the annual self-certification requirement can be viewed on Safe Harbor’s public website as being either “current” or “not current,” depending on whether the company failed to recertify within a reasonable time after its annual recertification became due. Further to that point, current policy is to remove a company from the Safe Harbor list if it fails to recertify within six to seven years. It is hoped that this due diligence requirement will be clarified in a few weeks at the July annual International Conference of Privacy Laws and Business in Cambridge, United Kingdom.

The other due diligence requirement that the Resolution seeks to clarify is that German data exporters must verify that their U.S. data importers are fulfilling their Notice obligations vis-à-vis the individuals, whose data are collected under the Principles. However, the Resolution does not specify the verification methods that the German data exporters should use.

The Resolution also requires German data exporters to develop and maintain records showing that they carried out the due diligence requirements that will be clarified in the Resolution. It may be required that proof of due diligence be presented to German data protection authorities upon their demand.

Should there be any concerns about a U.S. data importer’s compliance with the Safe Harbor after performing the due diligence required under the Resolution, German data exporters must instead use another approved method for transferring Personal Data to the U.S., such as binding corporate rules or standard contractual clauses.<sup>8</sup>

<sup>8</sup> Binding corporate rules (“BCRs”) is an internal system of governing privacy and data security that is better suited for a multinational organization than for a company that is located entirely within a single nation. To use BCRs for making transfers of Personal Data, a lead data protection authority must approve an application and a complete set of BCRs as well as any accompanying privacy policies and procedures. Only 7 companies have had their BCRs approved to date, as this method still entails a complex and lengthy approval process. Standard or model contractual clauses (“SCCs”) are designed for two-party/bilateral agreements. Three sets of SCCs have been approved for use by the EU (two sets for transfers between data controllers and one set for transfers between a data controller and a data processor). The provisions from a set of SCCs cannot be combined with provisions from another set of SCCs or partially selected to form a contract using a hybrid set or modi-

---

In addition, should the German data exporter find that a U.S. data importer's Safe Harbor certification is no longer valid or find that the U.S. company is not in compliance with any of the Principles, including the requirement to provide proper Notice to its data subjects, the German data exporter must notify the appropriate data protection authority.

### **Practical Implications**

German companies exporting Personal Data to U.S. companies that self-certify to the Safe Harbor should

---

fied set of SCCs. Each set of SCCs must be used in its entirety for any one contract, but other non-SCC provisions can be added to the contracts so long as they do not contradict the SCCs in any direct or indirect way. Approved SCCs are available on [http://ec.europa.eu/justice\\_home/fsj/privacy/modelcontracts/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm).

examine their policies and procedures to determine if their due diligence practices need to be modified as a result of the clarifications contained in the Resolution. Likewise, U.S. companies that self-certify to the Safe Harbor should be prepared to assist their German counterparties with their due diligence process when importing Personal Data from them. In the recent past, several data protection "scandals" have become public in Germany, affecting several of Germany's largest and most well-known corporations. Therefore it can be expected that German companies will strictly adhere to the Resolution, although the Resolution does not have the same effect as enacted law or a court decision. Failure to follow the clarified due diligence practices contained in the Resolution could, however, potentially lead to an enforcement action by German data protection authorities as well as reputation damage from unwanted media attention, which German and U.S. companies would want to avoid.