

ALERTS AND UPDATES

German Privacy Regulators Issue Decision on Data Protection and Safe-Harbor Self-Certification of US Companies

May 28, 2010

A recent decision of German regulators may make compliance with privacy protections more challenging for US businesses doing business in Germany. Germany operates a regional system of data privacy regulation where each *Länder* (or state) appoints its own regulator for the private sector. Those regulators try to adopt a common stance on issues affecting Germany through an informal organization known as the Düsseldorf Kreises.

At its last [meeting in Hanover](#) on April 28–29, 2010, the group reacted to concerns about problems with the transfer of data from Germany to the United States. A specific concern was the US Department of Commerce's Safe Harbor ("Safe Harbor") framework, one of the routes that enables data on individuals in Europe to be transferred to the United States. Safe Harbor has become an increasingly popular way of making data transfers lawful and is used by US corporations in connection with global HR systems, ethics policies, Sarbanes-Oxley reporting systems, transfers of customer details, social media operations and sales reporting systems.

Safe Harbor has encountered considerable opposition, including in a [report prepared by Australian consultancy Galexia](#) in December 2008. That report called on US and European Union authorities to increase policing of the program. The main objection was that a number of organizations professing to be registered under Safe Harbor were actually not registered. Galexia said that 1,597 corporations had self-certified, but only 348 met the basic requirements of the program. While it appears that some within the US Department of Commerce question some of Galexia's findings, the report has highlighted concerns about the framework.

The Düsseldorf Kreises has maintained that, as a result, corporations can no longer take a US organization's Safe Harbor self-certification as conclusive proof of adequate protection of personal data. In particular, Safe Harbor certifications more than seven years old should not be treated as valid. This last point appears to warrant clarification by local regulators since, in practice, Safe Harbor requires recertification every year. Parties dealing with a corporation on the Safe Harbor list may wish to independently check the certification and, in some circumstances, examine the policies and procedures behind that self-certification. In addition, the Düsseldorf Kreises called on the US regulator, the Federal Trade Commission, to step up its Safe Harbor enforcement program.

Given the indicated misgivings over the program, as well as the rising tide of concern over the transfer of personal data, regulators outside Germany are likely to closely monitor this issue. Any corporation that has self-certified under Safe Harbor—or relies on the certification of its business partners—may want to be aware of the possibility of more inquiries about the policies and procedures it adopts for holding, securing and transferring data.

For Further Information

If you have any questions this *Alert*, please contact [Jonathan P. Armstrong](#) in our [London office](#), [Sandra A. Jeskie](#) in our [Philadelphia office](#), any of the [members](#) of the [Information Technologies and Telecom Practice Group](#) or the attorney in the firm with whom you are regularly in contact.