



## DATA PRIVACY: MONTHLY HIGHLIGHTS

| DON HARRIS

More criticism of the U.S. Safe Harbor process emerged in July in Germany, with the [Data Protection Authority \(DPA\)](#) of the German state of Schleswig-Holstein calling for either an enforcement crack-down or the immediate termination of the program. The straw that broke the camel's back in northern Germany appears to be the imminent release of another critique of Safe Harbor by Galexia, an Australian consulting firm. Since the new [Galexia report](#) can be expected to add more fuel to the anti-Safe Harbor fire that has smoldered in Europe since the program's inception, it would be appropriate to maintain some perspective on these recent developments.

In the first place, Safe Harbor is not going away. Member states of the European Union remain legally bound to comply with the decision reached by the European Commission on July 26, 2000 regarding the adequacy of the level of protection afforded by the Safe Harbor program. No single DPA, or group of DPAs for that matter, has the authority to ignore or fail to respect this ten year-old decision.

Secondly, the call for due diligence by the Düsseldorfer Kreis (a working group of German State DPA's) is quite modest, particularly with respect to use of Safe Harbor in the employment context. Any serious effort by a U.S. employer to join Safe Harbor will involve working with European subsidiaries to prepare for the certification and to develop the employee notices that will be required. In other words, no "extra" due diligence of the sort specified by the Düsseldorfer Kreis will be necessary.

Thirdly, and perhaps most importantly, almost all of the criticism of Safe Harbor in the 2008 Galexia report – and probably this will be true with the upcoming study as well – arose from the equivalent of a desk audit of information on certification documents and public websites. Many lapses were found, for example, in companies failing to mention one or more of the Safe Harbor Privacy Principles in their privacy policies. However, this does not mean that the companies in question failed to respect those principles in their handling of transferred data. Desk audits,

after all, can only reveal procedural or technical lapses, not substantive ones. I would argue that the point of the Safe Harbor Program is to deliver privacy protection to affected data subjects, rather than to satisfy a checklist of formal requirements. While meeting these requirements should not be optional, no one has produced any evidence I know of showing that anyone has been affected or harmed by the technical lapses cited in the 2008 Galexia report.

Should these lapses be addressed and corrected? Absolutely. Should the Department of Commerce and the FTC do more to ensure conformance to the requirements of the program? Most certainly. It does appear that both agencies are finally becoming more involved in “raising the compliance offspring” they helped bring to life. But bear in mind that since most reputable Safe Harbor companies are already toeing the line, this is not the time to throw the baby out with the bath water. 🌐

*About the Author:* Don Harris is a Global Data Privacy Expert with Jeitosa and the President of HR Privacy Solutions. He has over 20 years of experience and is internationally known expert, author and speaker on HR data privacy issues. He can be reached at [don.harris@jeitosa.com](mailto:don.harris@jeitosa.com).