Anxiety Remains for U.S. Businesses Despite New EU Data Agreement

The new EU-U.S. data transfer agreement and changing EU data laws do little to alleviate concerns.

Ricci Dipshan , Legaltech News

February 5, 2016

Since the invalidation of Safe Harbor by a European Court in October 2015, many legal tech firms and businesses have been holding their breath waiting for new guidelines. But even with an initial agreement reached on a replacement for Safe Harbor, named Privacy Shield, the industry's hope for clarification may still be a long way's off.

"EU national privacy agencies are requiring greater details about the agreement, and by February 29, the EU commission is required to provide a better explanation of how this is going to protect EU data privacy rights," said Linda Sharp, associate general counsel of ZL Technologies. "Additionally, all participating EU countries need to approve the Privacy Shield before it can go into effect. I presume that is going to take a little while."

The delay puts many companies in the uneasy position of continuing their usual international business operations without any foresight on how upcoming regulations will affect them.

"Employees working at multinational companies are already communicating between the U.S. and the EU. For multinational companies, European data comes over on a regular basis," explained Sharp. "It makes one wonder if certain amount of that data is already subject to litigation and review because it's here."

"It's interesting because this is a perfect example of where the law hasn't caught up to the technology," she added.

Indeed, despite its regulations, EU law can be rife with ambiance and contradiction on the issue of data regulation and ownership.

Sharp pointed to the ruling by European Court on Human Rights in *Barbulescu v. Romania* in January 2016 as a prime example: "[This case] evolved around an employer's right to seize data created during company time. The company required an employee to open an email account to communicate with their customer base – he opened two email accounts, one business and one personal."

"They had a company policy that mandated that [employees] could only use company equipment during business hours, for business purposes. Thus, when they seized his personal and business emails, created during working hours, the company successfully argued that any emails created should have only been for company use and, as such, the company had a right to look at the information."

"This seems extremely inconsistent with the EU policies that we are seeing around the Safe Harbor and the proposed Privacy Shield," Sharp said, adding that the opinion's wholly different approach to data is one "that's more in line with the U.S. law… which is inconsistent with other EU privacy regulations. So in a sense, pick a policy."

One Directive, Many Laws

While the EU data laws are set to be updated around the same time as Privacy Shield comes online, Sharp is skeptical that new regulations will address one of the most fundamental and cumbersome issues with the continents data policies — "a combination of so many different countries and so many different rules."

What is difficult for U.S. businesses is "the fact that each nation has their own tweak—so which rules apply, where the employee works, where you are trying to collect the data from, or where the individual is from," she said.

This also runs parallel to the tricky issue of legal jurisdiction in the EU. "For example, a Belgium company may have employees that come to work there every day, yet walk across the street to go home at night to any one of the neighboring countries. Yet, the EU regulations are written such that the employee has the right to bring a privacy action where they reside," Sharp said.

"In a data breach, there could be several employees' data that is at issue, thus potentially opening the floodgate to litigation in multiple countries, with their version of the EU privacy laws. Thus, the U.S. Company could face litigation not where they agreed to do business, but in fact many other jurisdictions, potentially driving up the cost of doing business."

Sharp asserted the EU's policies are needlessly complex and a detriment to the business community and its consumers. "It's interesting, because the governments seem more concerned about this issue than the average consumer that uses any number of social media outlets on a daily basis. The governments have been creating these complex processes that make it harder for companies to do business in the first place."

What is needed, she added, is for "the EU need to consider a legitimate single policy, and eliminate each country's specific laws; they have to recognize it creates barriers to doing business. In the long run, these EU regulations may not be helping their countries' economic growth."
