EU Data Protection Reforms Put Cos. In Privacy Pickle

By **Allison Grande**

Law360, New York (October 30, 2013, 10:36 PM ET) -- The European Parliament last week passed a revised version of data protection reform legislation that adds restrictions that will make it all but impossible for multinational companies to comply with both European Union and U.S. privacy laws, leaving businesses with little choice but to continue their aggressive lobbying efforts, attorneys say.

The parliament's Committee on Civil Liberties, Justice and Home Affairs on Oct. 21 **easily approved** a draft version of a data protection regulation **proposed by the European Commission** in January 2012 to unify and strengthen the bloc's 1995 data protection directive.

The parliament's version adds several provisions to the commission's proposal — such as bigger fines for violators, stronger safeguards for data transfers to non-EU countries and heightened accountability measures — that widen the already substantial chasm between EU and U.S. privacy regimes.

"There's no question that the two sides are moving farther apart and that what works in the U.S. may very well not work in the EU," Proskauer Rose LLP attorney Jeremy Mittman told Law360.

The European Council tempered the parliament's action late last week, when it **concluded a two-day meeting** of EU member state leaders without committing to a deadline sought by the parliamentary committee, which wants to see the legislation finalized before the May 2014 European elections.

Still, attorneys anticipate that the delay will do little to derail the push to tighten the bloc's data protection regime, and that a structure that distances itself from the thin body of U.S. privacy law will be in place by early 2015.

"We are not much longer than a year away from a radical and wide-ranging legislative change that will affect data-reliant businesses more than anything seen until now," said London-based Field Fisher Waterhouse LLP partner Eduardo Ustaran.

Attorneys say companies should use the extra time created by the council's hesitance to push for a less restrictive regime that would better align with requirements in the U.S. and other jurisdictions.

"The regulation has been called the most-lobbied piece of legislation in EU history, and I'm sure that if the regulation would need to be picked up by a new European Parliament after the elections, companies will ... use the change as an opportunity to ensure that any messages that didn't get through last time get through a second time," said London-based Sidley Austin LLP partner William Long.

Multinational companies such as Google Inc. and Facebook Inc., which have already**launched aggressive lobbying campaigns** to ease some restrictions, may also have a better chance at getting their views across in the council, which has the reputation of being more business-friendly than the parliament, Ustaran added.

"In relation to privacy maters, the parliament has traditionally become a fierce advocate for the rights of citizens ... [while] the council tends to inject a dose of realism which is more aligned with the economic and political priorities of the EU member states," he said.

One provision that is likely to be the subject of intense lobbying efforts is a provision **recently added** to the regulation in the face of widespread concerns over U.S. intelligence-gathering methods that came to light through the leak of classified documents by former U.S. National Security Agency contractor Edward Snowden beginning in June.

The provision would bar multinational companies from handing users' personal data over to authorities based outside the EU, unless they receive permission from local data protection authorities or can show that the transfer comports with an existing data-sharing pact between the requesting country and the EU

or the member state.

The change would not only substantially stall litigation, regulation and investigations being conducted by international authorities that require information from the EU, but would also put companies in the undesirable position of having to comply with conflicting data transfer requirements.

“The proposal seems to be based on the position that data transfers would be subject to EU law above all else,” said London-based Mintz Levin Cohn Ferris Glovsky & Popeo PCmember Susan Foster. “It seems likely that there will be heavy lobbying by U.S. companies to avoid being put in the middle between U.S. and EU legal orders.”

But while lobbying could help, the damage done to the U.S.’ reputation by the Snowden disclosures has the potential to “weaken the hand of lobbyists that are pushing for concessions that would be beneficial to U.S. companies,” Mittman noted.

Companies are also likely to target other restrictions included in the draft passed by the European Parliament, including a new emphasis on biannual compliance reviews and the mandatory appointment of data protection officers for any company that processes information on more than 5,000 data subjects during a consecutive 12-month period.

“The appointment of a data protection officer is somewhat of an unfamiliar concept to U.S. companies, especially if they don’t have a large presence in the EU,” Mittman said, adding that basing the requirement on the number of data subjects a company has rather than how many people it employs will draw in many small- and medium-sized businesses unfamiliar with EU policy.

Companies are also likely to push for a return to the commission’s original proposal to give data protection authorities the power to assess fines of €1 million or 2 percent of a company's worldwide annual turnover, as opposed to the parliament’s proposal that the bar be set at €100 million ($136.7 million) or up to 5 percent of companies’ annual worldwide turnover, attorneys noted.

Even changes in the parliament’s draft that appear favorable to multinational companies could present challenges, attorneys noted.

While companies will likely prefer a mandatory notification period for data breaches of 72 rather than 24 hours and be OK with the requirement that they report to only one main data protection authority, the "one-stop-shop" notification requirement will still be layered on top of the reporting obligations that companies have in nearly every U.S. state.

“The one-stop-shop concept is now less clear-cut and therefore, less likely to work,” Ustaran said.

--Editing by Kat Laskowski and Chris Yates.