ACAMS | MONEY LAUNDERING.COM

As EU Advances Privacy Agenda, U.S. May See Reason for Concern

November 6, 2014 By Colby Adams

An expected strengthening of data privacy standards in Europe and elsewhere could hinder efforts by multinational banks to share information on suspicious clients with their foreign affiliates, say current and former U.S. officials.

Under a proposed regulation forwarded by the European Commission in 2012, EU member-states would adopt uniform measures to protect personal data, in part by requiring companies to notify citizens of how their information is used and, in some cases, to obtain consent before sharing such details.

Companies would also have to notify individuals and data protection authorities "without undue delay, where feasible within 24 hours" if information has been misplaced or abused, according to the draft. A final version of the regulation could grant a centralized agency the authority to permit banks and other companies to distribute information internally, or effectively leave such decisions up to individual governments.

At the same time, several countries outside of the continent are crafting similarly rigorous privacy rules without exceptions for banks seeking to share anti-money laundering (AML) data with foreign branches, according to Sarah Runge, director of the U.S. Treasury Department's Office of Terrorist Financing and Financial Crimes.

In recent years, the United Arab Emirates, Uruguay, Hong Kong, Brazil and other jurisdictions have adopted or introduced legislation, or amended existing rules, to block sharing of personal information of their citizens with jurisdictions that don't have similar data protection laws.

"It's not even a convergence anymore. It's a direct conflict between AML and data protection," said Runge, during a panel at the *ACAMS 13th Annual AML & Financial Crime Conference* in September. "The problem is that AML is risk-based and data privacy is rules-based, and bringing those two things together is proving impossible," she said.

How the EU's proposed regulation might affect international investigations will depend on how the economic bloc's member-states individually define "data," said Michelle Frasher, a visiting scholar at the University of Illinois' European Union Center.

"Simply speaking, the U.S. considers data to be property of the holder and legislates data protection in limited areas, while the EU designates privacy as a human right and ownership of all personal identifiable information is bestowed upon the individual," said Frasher, who is researching the topic for the Society for Worldwide Interbank Financial Telecommunication, or Swift.

At loggerheads

The problem of how governments should balance financial transparency with financial privacy isn't new, nor is it getting any better.

Following the 2012 disclosure that HSBC USA failed to properly monitor trillions of dollars in wires and bulk cash shipments from affiliates, banks with U.S. operations have sought to maximize the data they share enterprise-wide while at the same time lowering their exposure to compliance risks by terminating high-risk accounts, product lines and correspondent relationships.

Addressing HSBC's executive team during a July 2012 congressional hearing, Sen. Carl Levin (D-MI) repeatedly asked the bank to "make sure" that it reports sanctions-related information to affiliate banks, even when the institutions operate in countries with strict secrecy laws preventing such data-sharing.

The bank's $1.9 billion settlement forced global institutions to rethink how they pass along compliance information without violating the EU's 1995 Data Protection Directive. One such solution adopted has been to require clients to agree to limited data-sharing with overseas branches, *ACAMS moneylaundering.com* reported in November 2012.

Other financial institutions have relied on data-transfer agreements modeled on EU-approved contractual standards and have more recently turned to adopting a set of "binding corporate rules," or BCRs, according to Brian Hengesbaugh, a former U.S. State Department official who negotiated the Safe Harbor Privacy Arrangement with the European Union in April 2000.

Under the EU's current privacy directive, banks must submit their BCRs—effectively, plans for how to safeguard personal information—for approval from each nation in which they operate. The proposed regulation would require the institutions to submit new BCRs for approval within two years of its effective date.

The regulation as originally proposed mandates a single EU data protection authority, though lawmakers have endorsed an alternative plan that would empower agencies in each country to reject BCRs, possibly triggering a lengthy appeals process. The regulation would also significantly increase compliance penalties to the greater of $100 million euros or five percent of a company's global profits.

The current workarounds are "moderately useful" from a risk-management perspective because they allow for limited enterprise-wide risk assessments while

typically preventing the transfer of client information to third-parties, said Hengesbaugh, now an attorney with Baker & McKenzie in Chicago.

But the policies don't allow a U.S. bank, for example, to draft suspicious activity reports based on data it receives from a branch in the European Union, according to Hengesbaugh. The current workarounds "will, at the very least," have to be revised, in part because European outrage over global U.S. surveillance programs is likely to inform the final regulation, he said.

'A lot of problems'

In contrast to the EU's centralized data protection framework, the United States has promulgated different privacy standards for different sectors of the economy, at both state and federal levels.

"There are very few countries that are considered adequate by the EU, and the United States isn't among them," said Lisa Sotto, a privacy and cybersecurity attorney with Hunton & Williams in New York. New EU data privacy controls "could spell a lot of problems for a lot of companies, especially companies that don't qualify for safe harbor arrangements," she said.

Despite recent revisions, Financial Action Task Force (FATF) recommendations remain mostly silent on the topic, advocating for "the widest possible range of international cooperation" between financial intelligence units "consistent" with local data protection rules while making no mention of whether financial institutions should also distribute compliance data to branches abroad.

After acknowledging the issue in industry meetings, U.S. Treasury Department officials lobbied other FATF delegates to support increased sharing of know-your-customer data within a banking group, *ACAMS moneylaundering.com* reported in April 2013.

FATF guidance released last month notes that where cross-border data sharing "is restricted by, for example, censorship or data protection provisions, it will be difficult for banks to correctly identify [the risk of money laundering and terrorist financing] and therefore may fail to assess and mitigate it."