

EU lawmakers OK beefing up data protection laws (Update 2)

October 21 2013, by Juergen Baetz

A European Parliament committee on Monday approved sweeping new data protection rules that would strengthen online privacy and outlaw the kind of data transfers that the United States used for its secret spying program.

The draft regulation was beefed up after Edward Snowden's leaks about allegedly widespread U.S. online snooping to include even more stringent privacy protection and stiff fines for violations. The legislation will have significant implications for U.S. Internet companies, too.

After 18 months of wrangling and fierce industry lobbying, the legislation easily passed late Monday with a 49-3 committee vote, with one abstention. Parliament still needs to hold a plenary vote and seek agreement with the EU's 28 member states though—which is likely to result in some changes.

The rules would for the first time create a strong data protection law for Europe's 500 million citizens, replacing an outdated patchwork of national rules that only allow for tiny fines in cases of violation.

"Tonight's vote also sends a clear signal: as of today, data protection is made in Europe," said EU Justice Commissioner Viviane Reding.

Supporters have hailed the legislation as a milestone toward establishing genuine online privacy rights, while opponents have warned of creating a hugely bureaucratic regulation that will overwhelm businesses and

consumers.

"In the future, only EU law will be applicable when citizens' data in the EU will be used, independently of where the company using the data is based, be it in Germany, Ireland or the U.S.A.," said lawmaker Jan Philipp Albrecht, who led the negotiations on the legislation.

The legislation, among other things, aims at enabling users to ask companies to fully erase their personal data, handing them a so-called right to be forgotten. It would also limit user profiling, require companies to explain their use of personal data in detail to customers, and mandate that companies seek prior consent. In addition, most businesses would have to designate or hire data protection officers to ensure the regulation is properly applied.

Grave compliance failures could be subject to a fine worth up to 5 percent of a company's annual revenue—which could be hundreds of millions of dollars, or even a few billion dollars for Internet giants such as Google.

"Those companies are making billions from European citizens' data. So if you want them to comply, you have to give them the right incentives," said Giacomo Luchetta of the Center for European Policy Studies.

In response to the revelations of the National Security Agency's online spying activities, lawmakers also toughened the initial draft regulation, prepared by the European Commission, to make sure companies no longer share European citizens' data with authorities of a third country, unless explicitly allowed by EU law or an international treaty.

That means a U.S. tech companies would no longer be allowed to hand over private data of their European customers to U.S. authorities as they did for Prism, the secret spying program led by the NSA.

"Companies that still do it—if for example pressured by the NSA—will have to face drastic sanctions," lawmaker Albrecht said.

The provision will indeed protect European citizens from seeing their data transferred abroad for commercial purposes, but experts such as Luchetta caution that because of practical hurdles and loopholes, it might still be possible to transfer data on national security matters.

"If an American company gets a court order to hand over data, they have to comply," he said. "The U.S. court doesn't care whether you may be violating EU laws, and at the same time the EU has no power over U.S. court decisions."

In a move welcomed by consumer groups and businesses, the regulation also introduces a so-called one-stop-shop approach, meaning companies would only have to deal with the national data protection authority where they are based in the EU, not with 28 national watchdogs.

Consumers, in turn, would be able to file complaints with their national authority, regardless of where the targeted service provider is based. For example that would make it easier for an Austrian consumer to complain about a social media site such as Facebook, which has its EU headquarters in Ireland.

Meanwhile, the National Security Agency leaks continued to stir unrest among European policy makers.

French leaders appeared angry on Monday upon learning that NSA allegedly recorded 70.3 million French telephone records within a month, and called for a swift implementation of tough privacy rules to govern the tech sector.

"It is an important industry, but you cannot develop this industry if there

is no personal data protection," French Foreign Minister Laurent Fabius said in Luxembourg.

Fabius said French President Hollande also will push for the issue to be discussed at a summit of the EU's 28 leaders later this week in Brussels.

© 2013 The Associated Press. All rights reserved.

Citation: EU lawmakers OK beefing up data protection laws (Update 2) (2013, October 21)
retrieved 17 May 2024 from <https://phys.org/news/2013-10-eu-lawmakers-beef-laws.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--