GDPR Compliance Collides with U.S. Law at Supreme Court

Insights
3.07.18

The EU's General Data Protective Regulation ("GDPR") has been a popular topic of late. Fisher Phillips' Employment Privacy Blog has covered the evolution of this regulation, starting with the roll back of the previous "safe harbor" regime, as well as providing updates to GDPR compliance standards, and training recommendations.

As if to highlight the seriousness with which the EU is pursuing this directive, the GDPR has even made a recent appearance in Supreme Court arguments on Tuesday. *United States v. Microsoft*, No. 17-2, raised the issue of whether the United States may issue a search warrant to a U.S. based electronic communications service for data held on a server outside of the United States (in this case, Ireland). At the heart of the case is a 2016 ruling in favor of Microsoft and other tech companies by the 2nd Circuit limiting the geographic reach of the Stored Communications Act to data stored in the United States.

Among the many amicus briefs filed on behalf of Microsoft, was one submitted by the European Parliament, arguing that the US government must work through bilateral treaties in order to lawfully obtain the data stored in Ireland, or any other EU member country. The EU's position states that the "successful execution of the U.S. warrant would extend the scope of U.S. jurisdiction to a sizeable majority of the data held in the world's datacenters (most of which are controlled by U.S. corporations) and would thus undermine the protections of the EU data protection regime, specifically intended and designed to cover data stored in an EU Member State." With the EU having made its position clear, the Supreme Court's decision could set up a future conflict for companies seeking to comply with both U.S. and EU laws.

With the GDPR coming into full force on May 25th, and bringing with it steep new monetary penalties for violations, and with the EU's highest court having already weighed in, determining that EU law does not recognize the US legal regime as upholding Europe's "fundamental right to privacy," US companies with data stored overseas and/or European operations, should be following this case closely.

Employers should also have a training and compliance plan in place to prepare for implementation of the GDPR, which requires training on handling personal data. The EU's new website is a handy resource to start. GDPR compliance effects all levels of organizations which handle private information. With the enforcement data around the corner, organizations with any questions about

the applicability of the GDPR to their activities or how to prepare should contact their regular Fisher Phillips attorney or any of the attorneys in our Data Security and Workplace Privacy Group.

Related People

Robert Fallah
Attorney
610.230.2150
Email