Business Travel News

Master EU/U.S. Data Transfers or Simply Go with TMCs That Store Data in Europe?

By Amon Cohen / May 19, 2017

The Trump presidency is driving German businesses to end their contracts with travel management companies and other travel service providers that store their employees' personal data in the U.S., experts told BTN. Some German and Swiss companies have avoided service providers that transfer data to the U.S. ever since whistleblowing revelations from former U.S. National Security Agency contractor Edward Snowden during the Obama presidency. However, Dieter Koeve, an attorney with Koeve and Koeve, a law firm that advises German travel managers association VDR, said the trend has accelerated since Donald Trump assumed the U.S. presidency in January.

Koeve said German businesses are particularly spooked by Trump's Jan. 25 executive order, Enhancing Public Security in the Interior of the United States, which stated: "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."

Ironically, and in spite of initial concerns voiced by some European parliamentarians, the European Commission has stated that excluding European Union citizens from the Privacy Act does not conflict with the 2016 EU/US Privacy Shield framework. Privacy Shield, to which more than 2,000 U.S. entities have signed up, governs the transfer of data from the EU to the U.S. in a manner consistent with stricter EU data privacy laws, whereas the Privacy Act relates only to data generated within the U.S.

Nevertheless, the mood music behind the Privacy Act exclusion has been sufficient that "some companies have said to U.S. providers, 'We are not willing to work with you any longer,'" said Koeve. "The clear message I am hearing from more and more companies is that data storage must be here in Europe, and they have adopted new TMCs because their existing TMC was not able to fulfil their needs in Europe. In one case, a TMC told its client its main storage was in Europe but its back-up was in the U.S., and the client said, 'That is not compliant for us.'"

Also referencing Binding Corporate Rules, another mechanism by which companies can ensure compliant data transfers from non-EU countries to the EU, he continued: "Privacy Shield and Binding Corporate Rules are fine, but companies are suspicious of the new U.S. government. 'What do I do if an employee asks me where their data is stored?' I say it is stored under Privacy Shield in the U.S. Then they say, 'I read in the newspaper those guarantees are no longer relevant because President Trump signed an order that foreign citizens are no longer protected in the same way.' More

companies are saying it is too complicated and they want to be on the safe side. Privacy Shield is still secure, but you can only avoid discussion of this issue if you store data in Europe."

CTC Corporate Travel Consulting principal Jorg Martin sees the same trend among his clients. "The fear has dramatically increased that there might be misuse of data because Mr. Trump is saying so strongly he wants to put America first," said Martin.

Does What Happens in Europe Stay in Europe?

Acknowledging that some clients' policies forbid storage of data in the U.S., an increasing number of U.S.-based service providers have opened or expanded data facilities in Europe over the past couple of years. However, even in these cases, problems are arising. "We had a TMC which signed contracts saying all our clients' data would be stored in Europe, but we found out that its travel itinerary provider was based in the U.S.," Martin said. "The TMC hadn't mentioned that it used a subcontractor in the U.S. It meant that every booking was going there. Some of its clients stopped using the TMC because of that. This is a really big mess for the travel industry because TMCs use lots of subcontractors, such as data warehouses."

The need for EU companies to understand who has access to their data and where and whether it is handled compliantly is set to become significantly more pressing. The EU's General Data Protection Regulation, whose principles must be implemented by May 25, 2018, places a far greater burden on businesses to oversee protection of personal data, even if their contractors or subcontractors technically control the data and have primary responsibility. According to the U.K. Information Commissioner's Office, the GDPR also determines that "personal data may only be transferred outside of the EU in compliance with the conditions for transfer." Fines for breaches of the regulation will be as much as 4 percent of global turnover.