LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Meta's €1.2B EU Fine Raises Stakes For US Data Transfer Deal

By **Allison Grande**

Law360 (May 22, 2023, 11:06 PM EDT) -- European data protection authorities' record-setting privacy fine against Meta Platforms has left companies with limited options for transferring personal data from the European Union to the U.S., hastening the need for a new political agreement to permit these vital exchanges.

Ireland's data protection watchdog announced Monday that it had fined Meta Platforms Ireland €1.2 billion ($1.3 billion) for infringing the bloc's General Data Protection Regulation by sending European Facebook users' data to the U.S. using a mechanism known as standard contractual clauses without ensuring that adequate privacy safeguards were in place to protect the information.

Ireland's Data Protection Commission also ordered Meta to suspend any transfer of personal data to the U.S. relying on this framework within five months and to bring its data transfer operations into compliance with the GDPR within six months. These restrictions, coupled with the record-breaking monetary fine, are poised to have a significant impact on the future of transatlantic data flows for not only for Facebook parent Meta but also the wide range of companies who rely on these transfers to do business.

"This is a rare case of the fine being the least important part of the story," said Edward Machin, a London-based senior lawyer at Ropes & Gray LLP.

"The [Irish Data Protection Commission's] ruling that the standard contractual clauses are not a valid mechanism to transfer personal data to the U.S. will have a significant impact on the ability of organizations of all shapes and sizes to lawfully share and receive data from Europe," Machin said. "It will also kick off a race against time for lawmakers to finalize the EU-U.S. data transfer framework before the end of the six-month transition period that the DPC has given Meta to bring its transfers into compliance."

EU and U.S. policymakers announced in March 2022 that they had reached a deal to replace the Privacy Shield data transfer framework, which had enabled thousands of multinationals to legally transfer data from the EU to the U.S. but was struck down by the European Court of Justice in 2020 due to concerns over the framework's failure to provide Europeans with effective redress rights or adequately protect them from having their data intercepted by U.S. intelligence authorities.

While a key EU Parliamentary committee and national data protection authorities have issued nonbinding opinions advising against the adoption of the replacement data transfer framework,

the European Commission has given preliminary backing to the deal and is slated to soon adopt a final adequacy decision that would trigger the implementation of the pact.

In response to Monday's ruling, the European Commission said it anticipated that this new arrangement, known as the EU-U.S. Data Privacy Framework, would be "fully functionable by the summer."

"This will guarantee stability and legal certainty," the commission said.

It would also provide relief to Meta, given that it would negate the directive to halt data flows using existing mechanisms by the fall, as well as to other companies that are facing similar concerns about their data transfer procedures in light of the EU regulators' conclusions.

"There's been a recognition for quite some time now that this is a challenge that companies alone can't resolve," said Caitlin Fennessy, vice president and chief knowledge officer at the International Association of Privacy Professionals. "This decision ratchets up the risk and the temperature on these issues and drives home that a government fix is needed on these issues."

However, whether the new Data Privacy Framework will be enough to quell these concerns remains to be seen.

Industry group BSA-The Software Alliance called on the U.S. and EU to "quickly finalize" the new Data Privacy Framework, arguing that the deal would "increase trust in data protection and government access across borders."

"The agreement, once in place, will both improve privacy protections and provide greater certainty for EU-U.S. data transfers," said Aaron Cooper, vice president of global policy for BSA.

But consumer advocates continue to express doubts that the commitments U.S. officials have made to guard against unauthorized access by intelligence officials and to enhance consumer redress rights have gone far enough.

Max Schrems, the Austrian privacy advocate who spearheaded the legal challenges that led to the invalidation of Privacy Shield and its predecessor Safe Harbor framework, has already vowed to challenge the legality of the new Data Privacy Framework.

In responding to the enforcement action against Meta on Monday, which stemmed from a complaint he filed in 2013 with the Irish regulator challenging the company's data transfer practices, Schrems continued to insist that the new deal was unlikely to be a permanent fix.

"The simplest fix would be reasonable limitations in U.S. surveillance law," Schrems said. "There is an understanding on both sides of the Atlantic that we need probable cause and judicial approval of surveillance. It would be time to grant these basic protections to EU customers of U.S. cloud providers."

Alan Butler, executive director and president of the Electronic Privacy Information Center, or EPIC, agreed that it was hard to see how the Data Privacy Framework could withstand judicial review when the enhanced protections for how the U.S. intelligence community handles EU residents' personal data and fields government surveillance complaints came from the executive branch, rather than through Congress enacting a law.

"This is a hugely significant decision that really sets up the next phase in the resolution of EU-U.S. data transfers, which will be whether efforts in recent post-Privacy Shield negotiations provide sufficient protections in the long run, given that they're purely within the executive branch and not set by law," Butler said.

In its decision striking down Privacy Shield, which is known as Schrems II, the EU's Court of Justice declined the opportunity to invalidate standard contractual clauses that companies use to transfer personal data from the EU to regions such as the U.S. However, the high court advised EU data protection authorities to more carefully scrutinize transfers using the tool.

The European Commission in 2021 moved to update standard contractual clauses to align with Schrems II, providing companies with examples of possible "supplementary measures" that they may find necessary to undertake to transfer data in accordance with the high court's ruling, including encrypting transferred data.

However, in coming down hard on Meta in its newly announced decision, the European data protection authorities made it clear that the operational and technical safeguards that the company had taken to address concerns that transferred data could end up in the hands of U.S. intelligence authorities weren't enough to prevent this outcome.

While the decision won't halt all international data transfers, since they'll continue to be assessed on a case-by case basis, "it will put pressure on companies to think long and hard about their transfers to the U.S.," said Alex van der Wolk, a Brussels-based partner and co-chair of Morrison Foerster LLP's global privacy and data security practice.

"Suffice to say, it's going to make data transfers harder and not easier," van der Wolk said.

This will be especially true in the short term, as companies wait for the European Commission to finalize the replacement data transfer pact.

"We have a rocky few months ahead of us here," said Fennessy of the privacy professionals group. "That $1.3 billion price tag is going to scare people and is likely to lead some companies to decide to take more drastic actions or demand localization of their business partners."

Companies may also choose to take more measured steps such as enhancing the supplemental measures they have in place to support their data transfers.

EPIC's Butler noted that the decision announced Monday, along with the growing prevalence of state data privacy laws, ramps up the urgent need for companies to get a solid handle on what data they're collecting, where it's going, who has access to it and how it's being used.

"These are all questions companies have to ask when evaluating the risk of these data transfers," said Butler, adding that such considerations can play a big role in ensuring that data is being stored and handled in a way that's inaccessible to governments.

Meta said Monday that it plans to appeal the Irish regulator's decision, which was reached in conjunction with the EU's other data protection authorities and to "immediately seek a stay with the courts who can pause the implementation deadlines, given the harm that these orders would cause, including to the millions of people who use Facebook every day."

Companies will be keeping a close eye on that appeal, as well as the actions of the national data protection authorities moving forward. While Monday's fine didn't reach the scale of the $5 billion penalty that the U.S. Federal Trade Commission slapped Facebook with in 2019 for a series of privacy missteps, the GDPR has only been on the books for the past five years and regulators are demonstrating an increased appetite not only to assess fines but also to order business practice changes, which are often more cumbersome for companies to handle.

"GDPR enforcement is increasing, and the fines are increasing, and it's likely that we're going to see that trend continue," said Morrison Foerster's van der Wolk.

--Editing by Jill Coffey and Emily Kokoll.
