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

All Eyes On EU High Court Review Of Top Data Transfer Tools

By **Allison Grande**

Law360 (July 14, 2020, 11:20 PM EDT) -- Europe's top court is poised to decide on Thursday the fate of a pair of popular cross-border data transfer mechanisms, in a ruling that is expected to have sweeping implications for the way information flows out of the European Union and how regulators scrutinize these exchanges.

The European Court of Justice has been asked to determine whether EU citizens are adequately protected when companies use a tool known as standard contractual clauses to transfer personal data outside the bloc, particularly in light of concerns about the access that U.S. intelligence agencies may have to this information. The ruling could also address the validity of another vital data transfer tool, Privacy Shield, which has attracted similar criticisms but which the court hasn't been charged with addressing in the current dispute.

An adviser to the high court in December upheld the validity of both mechanisms while giving national data protection regulators broad leeway to block individual exchanges, and the Court of Justice is slated to follow up on that advisory ruling Thursday with a final decision that attorneys say could be a game-changer for data transfers from the EU to the rest of the world.

"This decision will be huge, because the court is examining two of the most widely used mechanisms for international data transfers, and whatever is said, whether it's good or bad or something in between, the implications will be very important," said Eduardo Ustaran, the U.K.-based global co-head of the privacy and cybersecurity practice at Hogan Lovells.

The dispute before the high court stems from a complaint that prominent Austrian privacy activist Max Schrems brought to Ireland's data protection authority in 2015, which challenged Facebook's reliance on standard contractual clauses to transfer data from the EU to the U.S.

During a virtual roundtable hosted by Hunton Andrews Kurth LLP's Centre for Information Policy Leadership last week, Irish Data Protection Commissioner Helen Dixon said she was eagerly anticipating the high court's decision for its potential to clear up confusion that's been swirling since the Court of Justice in 2015 invalidated Safe Harbor, another data transfer tool that was the predecessor to Privacy Shield.

In that decision, the court focused on whether EU law applies to citizens' data when it's accessed by public authorities in other jurisdictions but didn't get into other issues that the upcoming ruling is

expected to tackle, including what role regulators should play in policing these exchanges, according to Dixon.

"We're very much looking forward to Thursday because regardless of what the outcome is, we're going to avoid a lot of the legal uncertainty that has existed since 2015," Dixon said, adding that she was optimistic that the ruling would "give us the tools and the guidance to do whatever it is we need to do."

A Range of Possible Outcomes

While the Court of Justice typically follows at least some of the advocate general's advisory opinion, how the high court will ultimately come down on the validity of standard contractual clauses and Privacy Shield is far from certain, experts said.

In a press call hosted by the American Civil Liberties Union on Tuesday, complainant Schrems — co-founder of NYOB-European Center for Digital Rights — noted that Ireland's high court had referred 11 "very complicated" questions to the Court of Justice, making it "very unclear what the result is going to be on Thursday."

"It's not a black and white case where we say, 'Yes, [these mechanisms are] either going to live or die,'" Schrems said.

One scenario is that the Court of Justice could elect to go beyond what the advocate general has recommended and strike down standard contractual clauses on the grounds that the mechanism doesn't prevent the U.S. government and other third parties from broadly accessing this data and that EU citizens don't have adequate means to remedy this overreach.

"This [would be] the worst possible outcome for all businesses that transfer personal data outside of the EU," said Aaron P. Simpson, a privacy partner at Hunton and former managing partner of the firm's London office. "Their invalidation would be a significant blow to all businesses that rely on them, and would severely curtail the ability of U.S. companies to do business in Europe, and European businesses to use U.S.-based service providers."

Given that standard contractual clauses are widely used by both large and small companies to ensure that data is being transferred with the appropriate safeguards in place, striking them down would leave businesses scrambling to implement one of the few alternatives to send data not only to the U.S. but to any other part of the world whose data protection regime isn't on par with the EU's, experts said. They added that this process could be further complicated if the ruling allows for little or no transition time to overhaul their plans.

"If standard contractual clauses are no good anymore, a whole lot of companies are going to have a big problem," said Morrison & Foerster LLP privacy and data security group global co-chair Alex van der Wolk, who works in Brussels and London.

Companies could look to put in place binding corporate rules, but this isn't likely to be feasible for many organizations because they can only be used for transferring data within a corporate unit and require regulatory approval, which typically takes years to obtain.

The EU's General Data Protection Regulation also includes several exceptions, or derogations, that allow data to be transferred for certain purposes, including when consent is obtained or to defend against

legal claims. But those options are "limited in scope and generally unsuitable for routine data transfers," Simpson said.

"Organizations that are unable to implement an alternative transfer mechanism or rely on a derogation will be faced with a difficult decision: risk enforcement action or suspend data transfers until an alternative option is available," Simpson said. "Neither option is satisfactory, and both result in significant risk or disruption to business."

The best alternative to standard contractual clauses for most companies is likely to be Privacy Shield, which was instituted in 2016 to replace the invalidated Safe Harbor mechanism and is relied on by more than 5,300 companies. But that tool can only be used for data transfers from the EU to the U.S., and there's no guarantee that Privacy Shield will survive the Court of Justice's latest ruling, either.

"If Privacy Shield is struck down and standard contractual clauses continue, then U.S. companies in general can switch over to standard contractual clauses," said Peter Swire, a former White House privacy official and current senior counsel at Alston & Bird LLP. "But if standard contractual clauses and Privacy Shield go down, then there will be literally no lawful basis for most transfers of personal data from Europe to the U.S."

The advocate general acknowledged in his December opinion that the issue of Privacy Shield's validity wasn't directly before him. But he proceeded to spend 10 pages of the ruling laying out his concerns with the data transfer mechanism and skepticism of the European Commission's conclusion that U.S. surveillance law doesn't infringe the data protection rights of EU citizens whose information has been transferred under the arrangement.

"The advocate general drafted a road map for how to strike down Privacy Shield if the court wishes to do so," said Swire, who served on the U.S. team that helped negotiate the since-invalidated safe harbor agreement with the EU that took effect in 2000.

Given that Privacy Shield doesn't require companies to draft up legal-heavy contracts and allows them to instead focus on operationally adhering with certain privacy principles to safeguard transferred data, the program has been favored by many businesses, particularly smaller ones, that would be dealt a blow if the arrangement were to be shut down less than five years after being put into place, according to Hilary Wandall, senior vice president of privacy intelligence and general counsel at privacy compliance technology provider TrustArc.

While this move is widely seen as being unlikely, Wandall pointed out that few thought that Safe Harbor would be struck down in 2015. Additionally, if the Court of Justice elects to pass over the Privacy Shield question in this case, another challenge mounted by French digital rights group La Quadrature du Net that specifically challenges data transfers under Privacy Shield is scheduled to be heard and decided in the next year or two, Wandall said.

"If the court doesn't get to it Thursday, the expectation is they'll get to the Privacy Shield issue in the La Quadrature du Net case," she said.

At the other end of the spectrum, the Court of Justice could find both data transfer tools to be valid, which would be "the best outcome for all businesses that transfer personal data between the EU and countries outside the EU," Simpson said.

The high court could also stake out a middle ground by deciding to stick with the advocate general's opinion, which said that both mechanisms should be allowed to continue but that data protection authorities should have the ability to stop individual transfers that are deemed problematic.

This type of ruling would likely be welcomed by businesses, since it would allow them to continue using the data transfer tools. But it would also saddle companies with a "significant administrative and regulatory burden" if they're required to evaluate and verify case by case whether each individual data transfer provides an adequate level of protection for EU citizens' data, according to Simpson.

Schrems said Tuesday that his side also wouldn't necessarily object to such an outcome, especially if the ultimate result is that the specific Facebook data transfers that he's challenging are shut down.

"If you look at the net result, are data transfers stopped or not, it's not only about whether standard contractual clauses or Privacy Shield are invalid or not, but also why they're valid or not," Schrems said, adding that the mechanisms "may only be seen as valid because there's a solution within the system that still stops the data transfers."

What Happens Next

While invalidation of both mechanisms is certainly still in play, experts generally believe that a decision that hews closely to what the advocate general said is the most likely outcome.

"I don't think we're going to see everything will be invalidated and I don't think the court is going to say everything is fine, so it's likely to be something in between," Ustaran said, adding that given the range of issues and complexities involved in the case, "even if something small diverges from the advocate general's opinion, that could be quite shocking."

If the high court follows the advocate general's reasoning, companies that rely on standard contractual clauses to facilitate their international data flows will have to start doing more vetting of their transfers and exercise greater control over who has access to personal data being sent to their customers, clients, service providers and other third parties outside the EU, attorneys noted.

"Companies oftentimes enter into standard contractual clauses as a check-the-box exercise, but given the greater level of scrutiny that the advocate general is suggesting, companies that are sending this data out of the EU will need to focus more on the circumstances in which they're entering into these arrangements and do an appropriate risk analysis [ahead of time] to determine if that's the best way to transfer this data," TrustArc's Wandall said.

A ruling that embraces this middle ground would also ramp up the potential for companies to face liability under the GDPR, which gives national data protection authorities the power to issue fines of up to 4% of companies' global annual revenue.

"If the court says that data protection authorities have to do a better job, we should indeed expect to see more scrutiny taking place," said van der Wolk, who noted that regulators may be inclined to start asking companies about their cross-border data transfers when discussing other data protection-related issues with them, including when businesses report a data breach.

Andrea Jelinek, chairwoman of the collective of national regulators known as the European Data Protection Board and head of the Austrian data protection authority, said during the Centre for

Information Policy Leadership roundtable last week that she would be looking closely at how the upcoming ruling impacts the role of supervisory authorities.

"These challenges have to be tackled [and] these will be our duties whatever the judgment will be," she said.

The European Commission is also poised to play a vital role if standard contractual clauses are thrown out. The commission has been working to update the clauses to align them with the more uniform and stringent regime ushered in by the GDPR, which took effect in May 2018, and it's widely believed that the commission will be ready to issue the new set of clauses once the Court of Justice has issued its ruling.

"Depending what the court says, we could get the new clauses very soon," van der Wolk said. "Or if they have to go back to the drawing board, it may take a little more time."

Karolina Mojzesowicz, deputy head of the data protection unit at the European Commission, said during the roundtable that the commission would "scrupulously comply" with the Court of Justice's ruling and is "fully committed" to ensuring that data continues to flow and that transfer mechanisms are both "legally sound and viable long-term."

"We are already working on possible solutions and as necessary will intensify that work ... and take into account what our supreme court has told us," she said.

While experts are confident that international data transfers will continue no matter what the Court of Justice decides, what the court has to say about the U.S. government surveillance regime is poised to have long-lasting consequences on both foreign relations and the U.K.'s **bid to secure** a vital affirmation of its data protection standards before it leaves the EU at the end of the year, attorneys said.

"Based on all of my study, the U.S. has stronger safeguards for government surveillance than most or all of the EU member states, and Europe has not applied the same strict scrutiny to its own surveillance practices to date," Swire said, adding that the U.S. significantly strengthened these safeguards by curtailing certain bulk data collection activities by intelligence authorities with the passage of the USA Freedom Act in 2015.

Given that European privacy advocates have already expressed skepticism about the U.K.'s surveillance practices, "if the U.S. is held inadequate, the same process could readily apply to the U.K. after Brexit," Swire said. Additionally, a ruling that swings that way will also likely prompt questions about how the holding affects data sent to other countries like China, which have "drastically fewer protections against government surveillance than the U.S.," he said.

"The question is whether the court is really going to insist on these huge blockades on global data flows," Swire said.

--Editing by Breda Lund and Brian Baresch.