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

Data Transfer, Enforcement Questions Linger Post-Brexit

By **Allison Grande**

Law360 (January 26, 2021, 10:18 PM EST) -- Last month's trade deal between the European Union and U.K. will keep data flowing freely between the regions for now, but companies will have to keep watch for clarity in the coming months on how long this reprieve will last and how the U.K. data protection regulator will wield its new independence.

The Trade and Cooperation Agreement, announced Dec. 24, maintains the status quo of companies being able to transfer personal data from the EU to the U.K. without restrictions for an additional six months beyond the original expiration of the arrangement at the end of 2020.

The extension gives the European Commission a chance to decide whether to grant the U.K. an adequacy status that would prevent the U.K. from being declared a "third country" that companies in the EU can't transfer data to without putting in place a mechanism like standard contractual clauses.

"The end of that transition period in six months is the next big deadline, and the hope is that the EU recognizes the adequacy of our system before then and hopefully none of us have to write standard contractual clauses to transfer data to the U.K.," said Emma Drake, a U.K-based data protection lawyer at Bird & Bird LLP.

The U.K.'s departure from the EU also shakes up the region's data protection landscape, attorneys said.

While the U.K. has adopted a framework that's nearly identical to the EU's stringent General Data Protection Regulation, its split from the EU removes the U.K.'s Information Commissioner's Office from the collective of national data protection regulators that coordinate on cross-border enforcement efforts. That means that companies that are accused of broadly violating the GDPR could face fines from the EU member state regulator coalition as well as the U.K. regulator.

"While the Brexit deal is indeed helpful to set the basis for the future U.K.-EU relationship, from a data protection perspective, it is a far cry from the days when the U.K. was a member of the EU," said Eduardo Ustaran, who's based in London and serves as global co-head of the privacy and cybersecurity practice at Hogan Lovells. "The U.K.'s departure from the EU also marks a departure from key operational aspects of the GDPR."

U.K. Information Commissioner Elizabeth Denham addressed the current state of affairs in a blog post Friday, in which she committed to "developing a new regulatory relationship with European data

protection authorities, sharing ideas and data protection expertise and co-operating on enforcement actions where appropriate."

"As evidenced by our work globally, regulatory cooperation remains key to ensuring we can protect the public's personal data wherever it resides," she said.

Denham also touted the "important safety net" that the trade deal provides in allowing transfers from the EU to the U.K. to continue uninterrupted while the European Commission considers the U.K.'s application for adequacy.

"This is very welcome news and was the best possible outcome for U.K. organizations given the risks and impacts of no adequacy," Denham wrote. "This bridge contained within the TCA will provide a legally robust mechanism that can give U.K. organizations confidence to continue digital trade in the coming months."

Denham noted that the EU committed in a declaration alongside the trade agreement to "promptly" consider the U.K.'s adequacy decision, and data protection attorneys are cautiously optimistic that the commission will find before the new deadline that the U.K.'s version of the GDPR provides "essentially equivalent" protection for personal data as the rules that are in place in the remaining member states.

"There are already countries, like Uruguay, New Zealand and Israel, that don't have the same rules as the EU and have an adequacy decision," said Andrew Shindler, a London-based partner at Locke Lord LLP. "If the U.K. can't get an adequacy decision, then who would get one?"

However, as Denham recognized in her latest blog post, "there is no guarantee that the EU will grant the U.K. an adequacy decision."

The EU's decision is likely to hinge on its assessment of the U.K.'s mass surveillance regime and whether the protections in place for limiting U.K. spy agencies' access to EU citizens' transferred data are sufficient. This will be the first time these rules for government access to personal data will be closely scrutinized, since national security-related topics are one of the issues the European Commission has no say on when it comes to EU member states.

In managing digital data flows over the last two decades, companies have been primarily focused on complying with key laws like the GDPR and transfer arrangements like standard contractual clauses and the now-invalidated Privacy Shield.

But now that the flow of data from the EU to the U.K. is being put under the microscope for the first time, companies that are trying to make business decisions about global data transfers are having to confront an even more complex landscape, said Jim Koenig, who is based in the U.S. and co-chairs the privacy and cybersecurity practice at Fenwick & West LLP.

"Questions about surveillance and trade politics have started to mix in to make expectations around what data flows would be allowed and compliance requirements much more complicated," he said.

Denham advised in her post last week that companies "should continue to take sensible precautions for any eventuality" and pointed businesses toward details on her agency's website about "the safeguards businesses can put in place now, to ensure data continues to flow even without an adequacy deal."

The main way for companies to prepare for an interruption in the unrestricted flow of data from the EU to the U.K. is to put in place a sanctioned mechanism — likely either standard contractual clauses or more complex binding corporate rules — for legally transferring data from the EU to any other country that has yet to achieve adequacy status, including the U.S. They could then apply the mechanism to EU-U.K. data transfers if that becomes necessary.

Standard contractual clauses, which require the sender and receiver of data to enter into an agreement over how transferred data will be handled, are likely to be the most popular option. But this choice also has the potential to be tricky at the moment, given that the European Commission is currently beefing up standard contractual clauses in a process that's expected to be completed by the middle of the year.

"There's a perfect storm on the horizon, which is that the future of EU data flows to the U.K. is going to be decided approximately around the same time as the EU finalizes the new standard contractual clause forms," Koenig said. "So companies that need to update these contractual safeguards are waiting on those things to be solved."

This update will mark the latest adjustment that companies will have to make to their arrangements for transferring personal data outside the EU, following the European Court of Justice's invalidation of the Privacy Shield and its predecessor safe harbor, which both enabled companies to lawfully move data from the EU to the U.S.

"Many companies are becoming fatigued after several rounds of having to change their data processing contract provisions and addendums," Koenig said.

Attorneys who spoke to Law360 suggested that companies keep a close eye on the progress of the U.K.'s adequacy application and move to act in a few months if it doesn't look like adequacy will be granted before July 1.

"If companies haven't already taken steps to put in place standard contractual clauses, it's probably not the time to do that now, particularly given that there's more hope now that an adequacy decision will be issued," said Drake, the Bird & Bird attorney.

Companies also need to keep an eye on whether the U.K. moves to adopt the EU's revised standard contractual clauses or comes up with its own version, attorneys said.

And in either event, businesses should also look toward updating their existing transfer agreements in the near future to account for their enhanced obligations under the new standard clauses, which call for conducting more stringent risk assessments. Those assessments will need to "take into account the legal framework of the importing country, particularly with respect to surveillance measures, to ensure that the transferred data will be adequately protected," said Morgan Lewis & Bockius LLP partner Pulina Whitaker, who is based in London.

Once the clauses are finalized, companies will have a year to replace their existing contracts, Whitaker added.

Koenig said he's seeing companies insert "creative" provisions in these revised contracts. The agreements may, for instance, give companies several weeks to review changes required by the new clauses, particularly indemnification obligations between the parties, rather than becoming automatically enforceable.

Brexit also opens the door to questions surrounding how data flows between the U.K. and U.S. will work.

Almost immediately after the Court of Justice struck down the Privacy Shield agreement in July due to concerns over the unfettered ability of U.S. intelligence authorities to access EU citizens' transferred data, the European Commission and U.S. Department of Commerce announced that **they were in talks** to come up with a replacement.

Rhode Island Gov. Gina Raimondo, the Biden administration's pick to be the next Commerce secretary, reiterated this commitment during her U.S. Senate confirmation hearing Tuesday.

"As I understand it, the negotiations are going well, and should I be confirmed, it would be the top priority of mine to finish the negotiations swiftly and ensure there is a successor agreement that protects the interests of American businesses and provides for that transfer of data," Raimondo told lawmakers.

If the EU were to strike a new data transfer deal with the U.S., the U.K. would need to separately apply its own adequacy assessment, although it would be likely to largely adopt the EU's framework for data transfers as well, similarly to how Switzerland has done with both Privacy Shield and its predecessor safe harbor.

The U.K. is unlikely to proactively make its own arrangements with the U.S. in the short term, given the limitations on Britain's ability to strike deals during the transition period without consulting with the EU, attorneys said. But that doesn't mean it can't somewhere down the line.

"The U.K. now has powers to make its own adequacy decisions and could potentially recognize jurisdictions that the EU hasn't recognized as adequate," Drake said, although she noted that any discrepancy could potentially affect the U.K.'s own adequacy position.

While some companies may be hesitant to put in place any new accord for transferring data to the U.S., Koenig said some may change their minds if a new framework compares favorably to the revised contractual clauses.

"If the new form of Privacy Shield is available when companies are required to update their old standard contractual clauses to new formats next year, even though they may be reluctant, it may prove to be a less burdensome and more cost-effective option, which would certainly attract the attention of some chief privacy officers and others who are reluctant to head down the Privacy Shield road one more time," he said.

--Additional reporting by Alex Lawson. Editing by Aaron Pelc and Emily Kokoll.