akerman

Practice Update

French Court Provides Guidance on Data Transfer Safeguards and Sufficient Protections Against Access Requests from U.S. Authorities

April 22, 2021
1:00 AM UTC
By Christy S. Hawkins

In the wake of the Court of Justice of the European Union's (CJEU) decision in *Schrems II*, companies have had few real-world examples of how they can provide "supplementary measures" to protect personal data from overbroad access requests by public authorities. Going beyond advisories and FAQs, France's Conseil d'Etat recently issued an opinion that found sufficient "supplementary measures" were in place to protect personal data from public authority access requests, and discussed the measures that were key to its finding. The court's perspective is a must-read for companies struggling with the risks of international data transfers following *Schrems II*, and evaluates factors we can use to protect personal data from overbroad personal data access requests from public authorities – both to meet the standards of EU Supervisory Authorities and the data subjects whose personal data is in play.

Background

In July 2020, the CJEU decision in a case referred to the CJEU from the Irish Data Protection Commissioner, colloquially referred to as "Schrems

Related People

Christy S. Hawkins

Related Work

Data Privacy and Security

Related Offices

Atlanta
Dallas

II," had global implications for the transfer and processing of personal data subject to the EU's General Data Protection Regulation (GDPR). Specifically, one major point of *Schrems II* was the CJEU's invalidation of the EU-US Privacy Shield as an approved data transfer mechanism under the GDPR. Months later, in March 2021, U.S. Secretary of Commerce Gina Raimondo and European Commissioner for Justice Didier Reynders announced in a joint press statement that they had decided to intensify negotiations on an enhanced EU-U.S. Privacy Shield Framework. But the joint press statement said little else, and unless/until an enhanced EU-U.S. Privacy Shield Framework is adopted, businesses must continue to rely on other mechanisms to transfer personal data to the United States under the GDPR.

In the wake of *Schrems II*, many businesses have been left with more questions than answers – not only concerning if or when a new EU-U.S. Privacy Shield Framework will be adopted, but also whether transfers to the U.S. based on other data transfer mechanisms – including Standard Contractual Clauses – can be lawfully made consistent with the GDPR. Many are wondering whether lawful transfers are even possible in cases where the data processing is or might be subject to U.S. law. This question goes beyond the obvious situation where personal data of persons located in the European Economic Area (EEA) is transferred to or processed in the United States. What about data processing that may be subject to U.S. law because one of the data processors is a subsidiary of a U.S. company, even though the controller and processors are based in and processing personal data in the EEA? For at least this limited situation, France's highest administrative court, the Conseil d'Etat, has provided helpful guidance.

What Supplementary Measures Are Enough?

In a recent case, the French court examined a claim filed by professional associations against Doctolib, an e-health service company in Europe, seeking to

stop Doctolib's processing of personal data because one of Doctolib's data processors, AWS Sarl, is a subsidiary of U.S.-based Amazon Web Services. Doctolib is an online platform being used in France as authorized by the ministry of Solidarity and Health to schedule COVID-19 vaccinations. The data at issue was hosted by AWS Sarl, a subsidiary of U.S. company Amazon Web Services. The associations claimed that because AWS Sarl was a subsidiary of a U.S. company, it was subject to U.S. law and, even in the absence of data transfer to the U.S., may be the subject of an access request by U.S. authorities. The court referenced the *Schrems II* decision and found that although there was a risk of access by U.S. authorities, there were appropriate protections in place so that the data processing could still proceed lawfully under the GDPR. The court examined three factors in finding that the data processing at issue provided sufficient safeguards against access by U.S. authorities: (1) legal safeguards, (2) technical safeguards, and (3) administrative safeguards.

Legal Safeguards

In assessing the legal safeguards in place, the court evaluated the contract between Doctolib and AWS Sarl, and more specifically, AWS Sarl's contractual obligations if faced with an access request. Because the contract contained a precise procedure that AWS Sarl must follow in the event of an access request by a public authority, specifically requiring it to challenge access requests from public authorities, this procedure weighed in favor of finding sufficient safeguards to protect such data from being disclosed in response to an access request in the United States.

Technical Safeguards

The court also emphasized that Doctolib set up a device for securing data hosted by AWS Sarl – the data at issue was encrypted and the key was entrusted to a third party located in France to prevent data from being read by third parties. With

this measure in place, there was an added layer of protection against inquiries from public authorities.

Administrative Safeguards

The court further examined two administrative safeguards in place which strengthened the protections against potential access requests from U.S. public authorities.

First, the court noted that the data was limited to contact information and did not include medical information on grounds for vaccination eligibility. Under the principle of data minimization, the collection had been strictly limited to the information necessary to fulfill the purposes of the contract: identifying people and making vaccination appointments.

Second, the court noted that the data was only retained for a limited time. In furtherance of the storage limitation principle, personal data was kept for a maximum of three months after the date of the appointment and could be deleted online sooner by the persons whose personal data is involved.

Key Takeaways

While the French court's decision applies in a very limited context, there are some key takeaways that companies can utilize to better protect personal data transfers that are at risk following *Schrems II*. **First**, the parties here went beyond the baseline contractual guarantees to protect personal data from access requests by a public authority. When incorporating additional contractual safeguards, companies should have an eye toward procedures that either or both parties will follow in the event of a public authority's access request. **Second**, the parties evaluated practical technical measures to protect the data at issue from such a request. Here, the parties ensured that the encryption key was stored and retained separately from the encrypted data, and moving forward outside this specific case, there may

be other comparable technical solutions to achieve a similar goal. **Third**, the court evaluated administrative safeguards in place in furtherance of two core privacy principles: data minimization and storage limitation. Companies assessing administrative safeguards would do well to ensure they are implementing privacy by design, including the principles relating to processing of personal data set forth in Article 5 of the GDPR.

In any case, it is clear that a "check the box" approach to personal data transfers from the EU will not be sufficient to support data transfers going forward. This minimal approach won't satisfy regulators or data subjects that personal data is protected from overbroad government access requests. Rather, companies must thoughtfully evaluate the protections in place for transfers outside of the EU and consider supplemental measures that may be needed to safeguard personal information, and in particular, from access requests by public authorities.
