Franchisors Impacted by EU Limits on Personal Data Transfers to the U.S.

July 22, 2020

What Happened? On July 16, 2020, in *Schrems II*, the EU Court of Justice invalidated the EU-U.S. Privacy Shield mechanism. The EU Court of Justice struck down a similar program, the EU-U.S. Safe Harbor, in 2015. Over 5,000 companies, including many franchisors and franchisees, that self-certified for Privacy Shield with the U.S. Commerce Department may no longer rely on it for data transfers of EU personal data to the U.S.

So What? Franchisors may be in breach of vendor and other contracts to the extent they have agreed to fully comply with all relevant data privacy laws and they fail to be covered by an appropriate legal mechanism allowing for such cross border transfer of data. In addition, with Privacy Shield no longer available as a data transfer mechanism, there is potential risk of EU regulatory cease and desist orders to stop data transfer, and fines of up to 4% of a company's worldwide annual turnover or gross revenues.

How Does *Schrems II* Affect Franchisors? All franchisors with operations or activities in Europe need to consider the impact of this EU Court of Justice decision. The main EU privacy law, the General Data Protection Regulation (GDPR), applies to any franchise (regardless of where it is based) that collects or processes personal data from EU residents. U.S.-based franchisors that receive customer data from their EU franchisees must review what data they collect and for what purposes to see what new actions may be necessary to comply with the GDPR. A franchisor operating a worldwide customer loyalty program should review how the Schrems decision impacts their program. Franchisors may also need to reconsider their handling of personal data for existing and prospective EU franchisees.

Why Did this Happen? The transfer of EU personal data is limited to countries with "adequate" data protection safeguards in place. Due to the access of the NSA and other federal law enforcement to personal data in the U.S., the *Schrems II* Court has again held U.S. data protection to be "inadequate." Privacy Shield utilized an "ombudsperson" process to protect EU data privacy rights, but the Court questioned its independence and authority to make binding decisions on U.S. intelligence.

Is that All? No. *Schrems II* calls into question the viability of Standard Contractual Clauses (SCCs), far and away the most common EU personal data transfer mechanism in use. SCCs are EU-approved appendices that permit data transfer, but parties to a contract must adopt the clauses *verbatim*. In so doing, the parties

agree to EU jurisdiction and the technical data protection requirements in the clauses.

Are Standard Contractual Clauses Dead? Not yet. A case-by-case analysis now applies to SCC transfers. The *Schrems II* Court holds that EU exporters of data (or EU data regulators) must suspend SCC data transfers when the law of the recipient country "allows its public authorities to interfere with the rights of the data subjects to which that data relates." Given that the U.S. already falls into that category of countries, however, it appears that suspensions of SCC transfers to the U.S. may be imminent.

Does Franchisor Compliance with the California Consumer Privacy Act Help in the EU? Not really. Many franchise businesses are now complying with the data privacy requirements of the CCPA, but the EU Court's decision in *Schrems II* was based upon concerns over the reach of U.S. intelligence into EU personal data. Even under the CCPA's data privacy regimen, EU personal data remains subject to surveillance by the U.S. government.

What Should Franchisors Receiving EU Customer and Personal Data Do?

1. **Take stock of the Personal Data You Collect.** Only collect personal data that you actually need. The collection and processing of data that is of little or no value will only expose you to risks of noncompliance with data privacy laws and possible costs and damages resulting from any data breach.

   All franchisors on U.S. soil should take a close look at how they receive, process and store the personal data of EU citizens. Prepare to explain the actions you have taken to protect the data at issue. If your franchise business enrolled in Privacy Shield, keep up the data protection measures you adopted as part of the process. Implementation of those safeguards indicates a strong privacy program, as opposed to a check-the-box approach. Know what happens to the EU data you receive, and with whom you share it. If the collection of EU data does not serve a specific purpose, do not collect and store such data.

2. **Adjust Your Contracts and Manuals.** To the extent possible and appropriate, insert contractual language that accurately states what you do to comply with data privacy laws, including cross border transfer of data. In addition, review all data privacy guidelines described in operations manuals to ensure they correctly inform franchisees of your data privacy directives. Given that EU data regulators are likely to focus early enforcement efforts on the giants of the tech industry, businesses can use this time to craft robust "data transfer agreements" and "data processing agreements" to supplement Standard Contractual Clauses.

3. **Look at the Clouds.** Cloud services may help with transfers, but they are not a panacea. Amazon Web Services, Microsoft Azure and Google Cloud arguably serve as nation-less server farms that allow the processing of data in the cloud, as opposed to any particular country. There are two problems with this argument. First, a cloud is a collection of physical servers with physical locations. In fact, cloud services offer restricted geographic regions to their customers. See https://docs.aws.amazon.com/general/latest/

gr/rande-manage.html. Second, cloud services are not immune to requests, subpoenas or surveillance by U.S. intelligence.

Still, a cloud provider can be a powerful ally in your corner. Expect the cloud providers and other big tech to continue to push EU regulators to accept the "EU Cloud Code of Conduct," in the works since 2017. Unless and until the cloud itself becomes an accepted data transfer mechanism, the cloud providers will argue that they provide "adequate" safeguards. On the same day that *Schrems II* was issued, Microsoft sought to assure its cloud customers, noting "a settlement that enabled us to begin disclosing transparency reports about the number of U.S. national security orders we receive and established new policies within the U.S. government limiting the use of secrecy orders." https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/

4. **Consider Other Data Transfer Mechanisms.** *Schrems II* ended Privacy Shield and weakened SCCs, but Binding Corporate Rules (BCRs) and GDPR Article 49 "derogations" remain limited options.

   BCRs are internal rules that govern transfers amongst the same group of companies. EU data authorities consider BCRs on a company-by-company basis. The approval process is multi-layered, and can be costly and time-consuming. As with SCCs, inter-company BCRs covering data transfers to the U.S. may face heightened scrutiny given *Schrems II*'s inadequacy finding.

   Article 49 of the GDPR permits data transfers pursuant to exemptions ("derogations") in the absence of a valid transfer mechanism. For example, a derogation can apply if a data subject explicitly consents to the transfer, or if the transfer is necessary for the performance of a contract between the data subject and the controller. The European Data Protection Board interprets derogations narrowly, however, and they are not intended to be large-scale solutions to data transfers to the U.S.

5. **Hope for New Transfer Mechanisms.** The EU and U.S. could negotiate a new mechanism to replace Privacy Shield, but it is unlikely at this point. Article 42 of the GDPR contemplates the development of codes of conduct and certification mechanisms to provide appropriate safeguards for cross-border data transfers, but there is nothing concrete at present. Finally, the EU Commission has been working on new SCCs, and was rumored to have them ready for release had *Schrems II* invalidated SCCs. It is not clear when or if such new SCCs will issue.

6. **Consult With Your IT About Alternatives.** If the EU effectively shuts down all viable means of transferring personal data to the U.S. for processing, then you may need to examine the feasibility and economics of replicating or creating operations in the EU to process the data there or another country deemed "adequate." The topic warrants a spot on corporate medium- and long-range planning agendas.

7. **Remain Pragmatic.** If the EU data authorities are left to enforce *Schrems II* alone, then past experience indicates that the Big Tech companies will receive the brunt of regulatory action, leaving the EU with limited resources to police the vast volume of data transfers to the U.S. If EU data controllers read *Schrems II* and refuse on their own to transfer data to the U.S., however, then the commercial impact will be abrupt and significant.

What Comes Next? The status quo for personal data transfers out of the EU will not likely remain for long. The U.S. tends to get the heat and headlines in the EU, but all nations engage in data intelligence. EU countries surveille their own citizens, and it continues to be an issue for debate. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_en.pdf. Further, many countries are enacting data localization rules, requiring any personal data to be stored in-that country. China and Russia, among others, assert a right to engage in intelligence on data found within their borders.

At the end of the day, a political solution is necessary. The EU will need to consider surveillance and national security as important considerations to be balanced against privacy rights, and seek a pragmatic, agreeable solution to commercial data transfer. The United States may need to bolster their enforcement of data privacy rights of individuals. In the meantime, companies must take stock of what personal data they collect and for what purposes. If they must handle the personal data of EU residents, it is essential that they monitor this volatile legal landscape and implement processes that are appropriate for their unique uses of personal data.

For more information, contact Tedrick Housh, Michael Cohen, Gaylen Knack, Carl Zwisler, a member of our Global Privacy, Cybersecurity & Data Protection team or your Lathrop GPM attorney.