Data collection in the EU: troubled waters for U.S. companies

By Gary Kibel, Esq., and Zachary Klein, Esq., Davis+Gilbert LLP

FEBRUARY 25, 2022

The distance between the United States and Europe is approximately 4,000 miles, but when it comes to laws governing the treatment of online data collection and use, the gulf seems much wider and is growing.

The United States has always had a much different data privacy law regime than the EU. In the United States, there is no omnibus consumer privacy law on the federal level; rather, there are various sectoral laws dealing with issues such as health care, financial services and children's data and a wide variety of laws on the state level.

Meanwhile, the European Union's General Data Protection Regulation (GDPR), which took effect in 2018, is a comprehensive law that contains 99 articles and 173 recitals and applies to all member countries. The disconnect between the jurisdictions has always been challenging, and now recent developments have made compliance for U.S.-based technology companies even more difficult.

Standard contractual clauses

Pursuant to Chapter 5 of the GDPR, transfers of personal data to a country outside of the EU can only take place where that country ensures an adequate level of protection for the rights of EU data subjects. The European Commission (Commission) has deemed the U.S. to be inadequate under this standard. U.S. and EU regulators had negotiated formal programs to make cross-border data transfers to the United States GDPR-compliant. These programs allowed U.S. companies to register and self-certify compliance with a series of privacy principles. Once registered, the U.S. company would itself be deemed adequate in order to receive personal data from the EU.

The first program, the US-EU Safe Harbor program, was invalidated by the Court of Justice of the European Union (CJEU) in 2015 as a result of a lawsuit from privacy advocate Max Schrems who convinced the court that the program did not offer an adequate level of protection from U.S. surveillance activities for EU data subjects. The parties negotiated a replacement program, the EU-US Privacy Shield, and that program was invalidated by the CJEU as well in 2020 in the so-called "Schrems II" ruling.

In the absence of an adequacy decision, the GDPR requires that companies implement appropriate safeguards, including enforceable data subject rights and legal remedies. The most frequently used mechanism has been the Standard Contractual Clauses (SCCs) — a contract pre-approved by the Commission that establishes certain controls to safeguard data as per EU standards.

The United States has always had a much different data privacy law regime than the EU. In the United States, there is no omnibus consumer privacy law on the federal level.

The Commission issued updated SCCs in 2021, featuring a customizable design with different modules and optional clauses that constituted a major departure from earlier versions. However, these new SCCs went into effect after Brexit and were not grandfathered into the separate U.K. GDPR framework. The U.K. issued its own International Data Transfer Agreement (IDTA) for transfers from the U.K., and a separate IDTA addendum that will allow companies to use the new SCCs in connection with U.K. data transfers. Since the U.K. is no longer subject to rulings from EU privacy regulators, it is expected that this program will be widely adopted and remain valid for U.K. to U.S. transfers of personal data.

Transparency and consent framework

The free internet is largely supported by online advertising, and the ad tech industry relies upon the collection of data in order to inform targeted advertising. The more accurate and detailed the data, the more effective and valuable the advertising.

This industry occurs mostly out of sight from consumers as tracking cookies on websites and other data collection mechanisms collect behavioral data from most internet-connected devices to be shared amongst many parties in the ad tech ecosystem, which is then manipulated and turned into actionable data for ad targeting purposes.

Pursuant to the GDPR, there must be a legal basis to process personal data. Data collected via cookies and other tracking mechanisms is considered personal data. Therefore, in order to

comply with the GDPR, the industry needed to come up with a process to ensure that industry participants collected such data with a legal basis under the GDPR. This proved to be a challenge for ad tech companies operating in the background of publisher websites. As a result, the industry developed and coalesced around a system known as the Transparency & Consent Framework (TCF) developed and implemented by the trade association IAB Europe A.I.S.B.L. (IAB Europe).

The European Union's General Data Protection Regulation (GDPR), which took effect in 2018, is a comprehensive law that contains 99 articles and 173 recitals and applies to all member countries.

Nearly 800 companies are registered as vendors with the TCF. Under the TCF, when an internet user visits a publisher's site and sees a pop-up cookie banner and clicks to accept the banner, the user is believed to have consented to the collection of personal data via retargeting cookies. At that point, a "TC String" is generated and a cookie is placed on the user's device or an existing cookie is updated. The TCF passes the user's consent to ad tech and other companies in Europe, which then rely upon that consent to collect and share a user's personal data to deliver targeted advertisements based upon that data.

In February, the Belgian Data Protection Authority (DPA) announced its decision in a regulatory investigation into the TCF that was prompted by the Irish Council for Civil Liberties, a privacy advocacy organization. The Belgian DPA found that the TCF program, as currently operated, violates the GDPR.

In its ruling, the Belgian DPA held, among other things, that (i) IAB Europe is a data controller under the GDPR but is failing to meet its many obligations as a data controller and (ii) the user consents obtained are invalid because users have not given specific, informed and granular consent.

While the ruling only impacts IAB Europe, the implication is that all participants in the industry relying upon the TCF are using tainted data that has been collected through invalid means. IAB Europe was fined EUR 250,000, given two months to come up with an action plan to fix the shortcomings and then six months to implement that plan once it is approved by the Belgian DPA.

In the meantime, IAB Europe is appealing the decision, but that appeal does not stay the ruling. Therefore, the entire industry is in limbo waiting to see how this data can continue to be collected and used in a compliant manner.

Google Analytics

Recent decisions by the Austrian DPA and the French "Commission nationale de l'informatique et des libertés" (CNIL) have found that the use of Google Analytics by EU website operators violates the GDPR. These rulings, the first in response to 101 complaints filed throughout the EU by the non-profit advocacy organization NOYB, are projected to set off a surge of similar decisions from other EU regulators.

The Austrian DPA found that Google Analytics cookies used by an Austrian website allowed the collection and transfer of personal data to Google in the U.S., including user ID numbers, IP addresses, and browser settings. Moreover, the Austrian DPA found that the SCCs executed by the website operator and Google did not provide an adequate level of protection under the GDPR, as Google's proffered supplemental safeguards did not overcome the risk of U.S. surveillance activities identified in the CJEU's Schrems II ruling.

The CNIL, echoing these concerns, noted that data transfers to the U.S. lack sufficient regulation and present privacy risks for French website users, and that supplemental measures taken by Google were insufficient "to exclude the accessibility of this data for US intelligence services."

Conclusion

U.S. businesses are begging for a diplomatic solution to the cross-border data transfer issue since industry solutions are not working. And the ruling on the TCF strikes at the core of the ad-supported internet in Europe, a market dominated by U.S. companies. The next few months will be critical as more enforcement actions are likely, uncertainty in the industry grows and U.S. companies continue to sweat waiting for solutions to these many privacy challenges.

About the authors

Gary Kibel (L) is a partner at **Davis+Gilbert LLP**, where he is a member of the Privacy + Data Security and Advertising + Marketing practice groups. He provides clients perspective on cutting-edge issues in digital media, advertising, technology and privacy. He can be reached at gkibel@dglaw.com. **Zachary Klein** (R) is an associate in the Privacy + Data Security and Advertising + Marketing Groups. He helps companies meet their privacy and data security obligations and manage compliance risks. He can be reached at zklein@dglaw.com. The firm is located in New York.

This article was first published on Reuters Legal News and Westlaw Today on February 25, 2022.