The GDPR, SCCs, BCRs, and *Schrems*: Deciphering the Data Privacy Alphabet Soup

By Michael J. Cahalane, Andrew R. McConville, and Kyle W. Cunningham

Michael J. Cahalane and Andrew R. McConville are partners, and Kyle W. Cunningham is an associate, at Cetrulo LLP in Boston. They defend corporations in various litigation contexts and advise clients on risk mitigation strategies. Cahalane is a vice chair for the FBA's Corporate and Association Counsel Division.

The authors thank Professor Kevin R. Powers, J.D., founder and director of Cybersecurity Policy and Governance Graduate Programs at Boston College, for his contributions to this article.

Interpreting the increasingly complex and evolving array of data privacy regulations is a time-consuming and expensive undertaking for businesses and their counsel. Prior to *Schrems* and its progeny, over 5,000 American and European Union (EU) companies relied on the transfer frameworks developed by the U.S. Department of Commerce and the European Commission (i.e., U.S.-EU Safe-Harbor Agreement and the EU-U.S. Privacy Shield).[1] The invalidation of these mechanisms due to the U.S. government's alleged failure to create data privacy safeguards equivalent to that of the EU's General Data Protection Regulation (GDPR)[2] has burdened companies doing business in both the United States and the EU with high compliance costs as they scramble to implement Standard Contractual Clauses and/or Binding Corporate Rules. Due to the lack of clear guidance provided by the Court of Justice of the European Union (CJEU), U.S. businesses using EU personal data should consult with an experienced cybersecurity and data privacy specialist or retain counsel with a background in GDPR compliance to determine the best approach for their enterprise.

Introduction: What Is the GDPR?

Since becoming effective on May 25, 2018, the GDPR is and has been one of the strictest privacy and security laws on earth.[3] The GDPR replaced Directive 95/46/EC, which was the previous rule governing the processing and transferring of data from 1995 until 2018.[4] While both the GDPR and Directive 95/46/EC give the same general instructions and measures, the GDPR is more comprehensive and applies to all companies involved in personal data transfers concerning EU data subjects.[5] The GDPR, among other things, creates rights for natural persons regarding the processing of personal data and rules relating to the free movement of such data.[6] The GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject')."[7] The rights created by the GDPR include:

(1) The right to erasure (i.e., the right to be forgotten).[8]

(2) The right to know the categories of personal data being collected and who is receiving it.[9]

(3) The right to be informed of the appropriate safeguards taken by a third country or international organization when personal data is transferred to one.[10]

(4) The right to obtain from the controller without undue delay the rectification of inaccurate personal data.[11]

(5) The right, without undue delay, and within one month of the data controller receiving the request, to receive information on action taken regarding the personal information.[12]

The GDPR can create potentially high compliance and noncompliance costs for businesses, given its broad definition of identifiable data information. When the GDPR first took effect, it was estimated that larger companies budgeted an average of $20 million to $25 million for GDPR compliance, while smaller companies budgeted around $4 million to $5 million.[13] Moreover, the CJEU's striking down of EU-U.S. frameworks developed by the Department of Commerce and the Federal Trade Commission and approved by the European Commission has increased compliance costs and made it increasingly difficult for U.S. businesses to adhere to EU data security requirements.

National Security Data Collection: NSA's "PRISM" and "UPSTREAM" Program's Effect on U.S. Data Transfers

The *Schrems I* and *Schrems II* decisions directly respond to the revelations regarding the National Security Agency's data collection programs, code-

named "PRISM" and "UPSTREAM," which came to light after the Edward Snowden leaks.[14] Data collection and surveillance programs such as PRISM and UPSTREAM were created following Congress's passing of Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333. Section 702 created procedures allowing the attorney general and the director of national intelligence to authorize jointly, for up to a year, the targeting of certain individuals reasonably believed to be located outside the United States in order to acquire foreign intelligence information.[15] Section 702 of FISA limits government surveillance to non-U.S. residents and for conversations occurring outside the United States, preventing parties targeted by data surveillance programs from asserting Fourth Amendment protections.[16] Similarly, Executive Order 12333 grants the NSA power to access data "in transit" to the United States by accessing underwater trans-Atlantic cables and collecting the data before it arrives to the United States and becomes subject to FISA.[17] In an attempt to assist American businesses with EU data privacy requirements, the United States developed the U.S.-EU Safe Harbor Framework in 2000, and later the EU-U.S. Privacy Shield in 2016.[18] The European Commission approved both; however, they were later struck down by the *Schrems* decisions.

In 2013, plaintiff Maximilian Schrems, an Austrian resident and a Facebook user, filed a complaint against Facebook Ireland, claiming that U.S. law and practices offer no real protection of the data kept in the United States against government surveillance due to the existence of PRISM and Facebook's participation in it ("*Schrems I*").[19] On Oct. 6, 2015, the CJEU found in favor of Mr. Schrems, declaring invalid the U.S.-EU Safe Harbor principles that U.S. businesses then used to comply with EU data privacy requirements.[20] In response to *Schrems I*, the U.S. Department of Commerce and the European Commission developed the U.S.-EU Privacy Shield, which imposed stricter requirements on U.S. businesses.

In 2020, building off *Schrems I*, a second CJEU decision, *Schrems II,* invalidated the EU-U.S. Privacy Shield, citing as grounds for its ruling the Presidential Policy Directive 28 (PPD-28) and FISA. Specifically, the court found that section 702 of FISA "does not indicate any limitations on the power it confers to implement surveillance programs for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programs."[21] Moreover, the CJEU found that PPD-28, a 2014 directive issued by the Obama administration to establish additional limitations on bulk signal intelligence collections,[22] "does not grant data subjects actionable rights against the US authorities."[23]

The CJEU found that Standard Contractual Clauses, or SCCs, remain a viable option for EU-U.S. data transfers.[24] SCCs are a set of pre-written clauses and conditions followed by both the sender and receiver of personal data that allow transfers of data to countries outside the EU.[25] SCCs place the burden of data protection on the controllers and operators who would seek to transfer information.[26] The CJEU indicated that the entity transferring the data must ensure that the subject is afforded a level of protection equivalent to that guaranteed by the GDPR, and if it is not, there must be additional measures taken to compensate for the legal systems or protections afforded by a third country.[27] Since the CJEU has consistently found that the United States lacks adequate protections due to the country's mass surveillance system, parties engaging in EU-U.S. transfers must ensure that they are taking additional measures to protect EU personal data. While the CJEU explicitly rejected the Privacy Shield, it provided no practical guidance for developing adequate data protections compliant with the GDPR.[28]

On March 25, 2022, the European Commission and the United States announced that they have agreed "in principle" on a new Trans-Atlantic Data Privacy Framework to reconcile U.S.-EU data transfers in light of *Schrems II*.[29] To date, the new agreement has not been formalized into a binding legal document.[30] Moreover, Mr. Schrems has indicated that he is prepared to file suit a third time if the proposed Trans-Atlantic Data Privacy Framework is not compliant with EU data privacy laws.[31] Until the proposed Trans-Atlantic Data Privacy Framework takes legal effect, companies must still operate using existing data transfer methods and should be cautious moving forward in relying on transfer frameworks.

Without U.S. Data Transfer Frameworks, Companies Must Rely on Standard Contractual Clauses and Binding Corporate Rules

Standard Contractual Clauses

The CJEU, in *Schrems II,* explicitly upheld the use of Standard Contractual Clauses to transfer personal data from the EU to the United States; however, companies relying on SCCs are solely responsible for determining that U.S. law provides the same protections under EU law and are required to use additional safeguards to supplement U.S. law where appropriate.[32] In response to this requirement, on June 4, 2021, the European Commission announced the adoption of two new sets of SCCs: one for use between controllers and processors and one for the transfer of personal data to third countries.[33] Businesses that are controllers or processors of personal data can still continue to rely on the earlier Standard Contractual Clauses for contracts concluded before Sept. 27, 2021, as long as the processing operations that are the subject matter of the contract remain unchanged.[34]

Businesses in the United States using EU personal data should consult with an experienced cybersecurity/data privacy professional or a lawyer specializing in GDPR to ensure that their use of SCCs and other contractual clauses for data transfers complies with the regulation. Businesses should also monitor the European Data Protection Board as it continues to release additional guidance on the changing GDPR compliance requirements.

Binding Corporate Rules

Multinational corporations acting as data controllers within the EU should consider developing Binding Corporate Rules, or BCRs, for transfers outside the EU.[35] BCRs can be used by "a group of undertakings, or a group of enterprises engaged in a joint economic activity."[36] BCRs allow international transfers from the EU to organizations within the "same group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers of personal data."[37] These rules must also be legally binding and enforced by every member of the group. [38] For multinational corporations with an EU presence, BCRs offer several advantages to relying on SCCs for transfers of user data, including increased flexibility because a supervisory authority does not need to approve nonmaterial updates to BCRs.[39] Similarly, BCRs can be easier to maintain, as they create readily accessible uniform compliance requirements across the enterprise as opposed to intergroup contracts using SCCs.[40]

To be effective, BCRs must be approved by the supervisory authority responsible for enforcing the GDPR in the corporation's

European Economic Area Member State.[41] When developing BCRs, a corporation must specify:

1. "the structure and contact details of the corporation;
2. the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected, and the identification of the third country or countries in question;
3. how the rules are legally binding in nature, both internally and externally;
4. the application of the general data protection principles and the requirements for transfers to bodies not bound by the binding corporate rules;
5. the rights of data subjects and details regarding compensation for a breach of the binding corporate rules;
6. the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules;
7. the tasks of any data protection officer designated by Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;
8. the complaint procedures;
9. the mechanisms within the group of undertakings or group of enterprises engaged in a joint economic activity to ensure compliance with the binding corporate rules;
10. the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
11. the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (9);
12. the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and the appropriate data protection training to personnel having permanent or regular access to personal data."[42]

Multinational corporations acting as controllers of EU data who transfer information to the United States could benefit from implementing BCRs, particularly if they already have a robust in-house legal team and experienced cybersecurity and data privacy professionals trained in GDPR compliance. Such companies should re-evaluate their BCRs following the passage of any major U.S. or EU cybersecurity law implicating EU personal data to ensure that the protections for EU data subjects provided by their BCRs are still adequate under EU law. Additionally, multinational companies using BCRs should review their rules immediately following the acquisition, divestiture, or formation of any corporate entities, members, or affiliates to ensure that the new additions to the enterprise have internal procedures for handling EU personal data consistent with their existing BCRs.

Consequences for Violating the GDPR

Despite the lack of clear guidance from the CJEU following the invalidation of the EU-U.S. data transfer frameworks, businesses using EU personal data must become compliant with the GDPR or risk facing significant penalties. The consequences for failing to adhere to the GDPR can be harsh depending on the severity of the violation. Under Article 83(5) of the GDPR, fines can reach €20 million, or 4 percent of the company's global revenue, whichever is greater.[43] EU data protection authorities have been enforcing the GDPR with increasing scrutiny. The EU has issued 1,003 fines since July 2018, totaling €1.575 billion. Sector exposure has been highest in industry and commerce (224 fines totaling over €776 million) and media, telecommunications, and broadcasting (176 fines totaling over €596 million).[44] Countries issuing the highest number of fines are Spain (387), Italy (123), and Romania (73).[45] As a result, companies operating within these sectors or engaging in data transfers from these countries should proceed with heightened caution. In response to the harsh fines associated with violating the GDPR and lack of clear guidance from the EU, businesses have begun threatening to pull products relying on EU personal data. In its annual report issued on Feb. 2, 2022, Meta Platforms, Inc., the parent company for Facebook and Instagram, stated that if a new data transfer framework is not adopted and if Meta is unable to continue to rely on SCCs or another alternative means for transferring data from the EU to the United States, it will be unable to offer a number of products and services in Europe, including Facebook and Instagram.[46]

Conclusion

The NSA's surveillance programs have made compliance with the GDPR particularly difficult for companies doing business in both the United States and the EU. The PRISM and UPSTREAM programs remain in effect, with no signs of imminent repeal. Consequently, the U.S. Department of Commerce will likely face significant obstacles in creating a new Trans-Atlantic Data Privacy Framework. Since the CJEU has already declared invalid two adequacy decisions issued by the European Commission regarding prior U.S.-EU data transfer frameworks, companies utilizing EU personal data should exercise increased vigilance, given the CJEU targeting of EU-U.S. data transfers. As a result, at a minimum, it is imperative that companies consult with cybersecurity and data privacy experts to evaluate all data transfers and to identify ones that contain personally identifying information of EU citizens. When a U.S.-based business expects to receive personally identifying information from EU citizens, it should immediately refer the issue to an attorney specializing in U.S.-EU GDPR compliance. Multinational corporations based in the EU and transferring data to the United States should consider developing BCRs to help increase the efficiency of interorganizational data transfers.

A new Trans-Atlantic Data Privacy Framework and the inevitable challenges thereto, including a potential "*Schrems III,*" could reshape the already complex data privacy landscape. Until then, understanding SCCs and BCRs and relying on qualified professionals for advice are imperative for companies to make sense of the *Schrems* alphabet soup and avoid costly consequences. ⊙

Endnotes

[1]*Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., ECLI: EU:C:2020:559 (July 16, 2020),* 134 Harv. L. Rev. 1567,

continued on page 14