DrinkerBiddle

Client Alert

October 6, 2015

CJEU Declares Safe Harbor Framework Invalid

Overview

In a decision with significant potential ramifications for flows of personal data from the European Union to the United States, the Court of Justice of the European Union (CJEU) today ruled in *Maximillian Schrems v. Data Protection Commissioner* (C-362/14) that the Safe Harbor Framework no longer provides adequate protection for data transferred to the United States. The decision is likely to leave the over 4000 companies that are currently self-certified to the Safe Harbor Framework scrambling to put in place alternative legal mechanisms to enable trans-Atlantic data transfers to proceed.

Key Takeaways

- The Court found the EU Commission's decision approving the Safe Harbor to be invalid, citing the Commission's failure to determine that the totality of US laws and regulations provide adequate data protection to EU citizens.
- The opinion permits member state data protection authorities to independently investigate complaints related to countries that the Commission has deemed to provide adequate levels of data protection
- Data protection authorities could bring cases requesting that Commission adequacy decisions be vacated by the European Court, but data protection authorities could not invalidate a Commission decision without court action.
- The Court's opinion follows the rationale put forward by Advocate-General Yves Bot in his non-binding opinion issued on 23 September. (See our summary of the Bot opinion at http://www.drinkerbiddle.com/resources/publications/2015/safe-harbor-framework-under-stress.)

Next Steps

The Drinker Biddle & Reath Privacy and Data Security team continues to monitor developments in Europe and advise clients regarding next steps. The Drinker Biddle team will be holding a series of webinars and roundtables to review this opinion with clients and discuss options for the future. A general webinar and discussion will be held on October 13, and additional conversations will be scheduled. To be included in these conversations, please contact your Drinker Biddle lawyer or one of the lawyers listed below:

- Peter Blenkinsop – Peter.Blenkinsop@dbr.com
- Mary Devlin Capizzi – Mary.DevlinCapizzi@dbr.com
- Stan Crosley – Stanley.Crosely@dbr.com

For general information about our upcoming events, please contact Debbie.Armstrong@dbr.com.

Background

Max Schrems lodged a complaint in 2013 with the Data Protection Commissioner of Ireland concerning the fact that Facebook Ireland Ltd keeps its subscribers' personal data on servers located in the United States. Mr. Schrems claimed that revelations concerning the US intelligence surveillance program demonstrate that the law and practices of the United States offer insufficient protection of personal data. The Commissioner refused to investigate the complaint on the grounds that Facebook Ireland lawfully transferred personal data to the US pursuant to Facebook USA's self-certification to the Safe Harbor Framework, and that the Framework has been found by the European Commission under the Data Protection Directive (95/46/EC) to provide an adequate level of data protection of personal data transferred (Decision 2000/520). The Commissioner took the view that he was bound by such adequacy decisions, which are authorized pursuant to Article 25(6) of the Directive. That paragraph reads in part: "The Commission may find . . . that a third country ensures an adequate level of [data] protection. . . . Member States shall take the measures necessary to comply with the Commission's decision."

Mr. Schrems brought proceedings before the Irish High Court for judicial review of the Commissioner's decision. The High Court decided to stay the proceeding and to refer the case to the Court of Justice of the EU for a preliminary ruling on the question of whether the Data Protection Commissioner is absolutely bound by Commission adequacy determinations or whether the Commissioner can conduct his own investigation into the matter.

CJEU Opinion

Sitting as a Grand Chamber of 15 Judges[1], the CJEU opined that the independence of Member State data protection supervisory authorities is an essential component of the effective protection of personal data. Article 8(3) of the EU Charter of Fundamental Rights establishes that "[c]ompliance with [rules for the protection of personal data] shall be subject to control by an independent authority." The Charter is at the highest level of hierarchy of EU law, and according to the Court, it follows from Article 8(3) that a data protection authority (DPA) must always retain its power to investigate a matter, even when the Commission has adopted an adequacy decision under the Data Protection Directive. Examining Article 28 of the Directive, concerning the powers of DPAs, the Court found that the power to independently investigate complaints and to intervene to suspend processing (including transfers) where there is the risk of a breach of fundamental rights, like the right to protection of personal data, must be interpreted broadly. As a result, a Commission decision as to the adequacy of data protection in a third country should be viewed as having a binding effect, but national DPAs retain the power to investigate complaints. However, the Court explained that national DPAs lack the authority to declare Commission decisions invalid. If, after examining a data subject's complaint about the adequacy of a country's legal regime, the DPA believes the country does not provide an adequate level of data protection, the DPA must bring its argument to the national courts. The national courts should then, if they agree with the DPA, make a request to the CJEU for a preliminary ruling on the validity of the Commission's decision.

Having answered the question referred to it by the Irish High Court, the CJEU still felt obliged to give a "full answer." Accordingly, the CJEU proceeded on its own motion to examine the validity of the Safe Harbor Framework. Expounding on the criteria for an adequacy decision, the Court stated that an assessment that a third country ensures an adequate level of data protection requires making a finding that the level of protection in that third country is essentially equivalent to that afforded by the Data Protection Directive, even though the manner in which that protection is implemented may differ from the approach in the EU. This requires examining the third country's "domestic laws or international commitments and the practice designed to ensure compliance with those rules." Moreover, adequacy decisions must be periodically reassessed, particularly when new circumstances are brought to light that call into question a prior assessment. Although the Court felt that a system of "self-certification" could be acceptable, it noted that "the reliability of such a system . . . is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules . . . to be identified and punished in practice."

1 The Court of Justice is composed of 28 Judges appointed by the EU Member States. The Court may sit as a full court, in a Grand Chamber of 15 Judges or in Chambers of three or five Judges. The Court sits as a full court where prescribed by statute and in cases of exceptional importance. The Court sits in a Grand Chamber in cases of particular importance, or where a Member State or institution is a party to the proceedings and makes such a request. Other cases are heard by Chambers of three or five Judges. Decisions of the Court are taken by majority vote and no record is made public of any dissenting opinions.

Applying the above criteria to the Safe Harbor Framework, the Court began by noting that the Safe Harbor did not apply to "public authorities" in the United States. The Court also took note of the derogations to the Safe Harbor Principles that allow the Principles to be limited, as necessary, to meet national security, public interest, and other purposes of the United States government. This led the Court to conclude that the Safe Harbor enables interference with the principles of respect for privacy and protection of personal data enshrined in Articles 7 and 8 of the Charter of Fundamental Rights. The Court then took note of communications by the European Commission, which found that US authorities "were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible . . . with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security." Accordingly, the Court determined that United States law provided for access to personal data by government authorities beyond what is "strictly necessary," and that an EU data subject had no effective means of pursuing "legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data." Most importantly, the Court found that the Commission never engaged in a wholesale examination of US laws to determine whether their application, in combination with an organization's commitment to comply with the Safe Harbor Framework, would ensure an adequate level of data protection of transferred data, and concluded that the Commission had never determined that the United States ensures "an adequate level of protection by reason of its domestic laws or its international commitments." Accordingly, without engaging in any examination of the Safe Harbor Principles, the Court deemed the Safe Harbor "invalid."

Business Implications and Speculation About Schrems 2.0

The immediate and most obvious impact of the Court's decision is that companies that rely on the Safe Harbor Framework for transferring personal data from the EU to the US will need to swiftly implement alternative mechanisms for the transfer of the data. Article 26(1) of the Data Protection Directive provides a list of derogations to the restrictions on transferring personal data outside of the EU. These include:

Where the individual has given his unambiguous consent to the transfer;

- Where the individual has given his unambiguous consent to the transfer;
- Where the transfer is necessary for the performance of a contract between the individual and the data controller;
- Where the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the controller and a third party;
- Where the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; and

- Where the transfer is necessary in order to protect the vital interests of the data subject.

Nevertheless, it must be understood that the Working Party of EU data protection authorities (the "Article 29 Working Party") has narrowly construed these derogations. For example, in the employment context, consent is rarely viewed as valid due to the imbalance in the relationship of the parties. "Legal claims" is typically interpreted as meaning claims arising under Union or Member State laws. "Important public interest grounds" is often viewed as applying only where such interests are established in Union or Member State law.

In addition to the derogations found in Article 26(1), Article 26(2) of the Directive allows international transfers to take place to recipients in jurisdictions that have not been deemed to ensure adequate data protection where the controller implements adequate safeguards approved by the relevant Member State. Pursuant to Article 26(4), this may include certain standard contractual clauses approved by the Commission, and it has also been interpreted to include the implementation of binding corporate rules (BCRs) that govern the transfer of personal data among affiliates of a multinational corporation, where such BCRs have been approved by relevant DPAs. Given that the timeframe for development, implementation, and approval of binding corporate rules typically takes at least 18 months, the quickest option is likely to be the execution of the standard contractual clauses (controller-to-controller clauses and/or the controller-to-processor clauses). Depending on the number of EU legal entities from which data needs to be transferred and the number of US recipient entities, the complexity of doing so will vary. Moreover, for multinational companies whose approach to global data transfers from the EU has in the past relied upon first exporting personal data to the US and then using onward transfer agreements to transfer the data elsewhere, the burden of putting in place the necessary agreements could be significant. It must also be remembered that in some EU Member States, the use of standard contracts must be notified to the relevant data protection authority, and if sensitive personal data is involved, DPA prior approval may be required. Other challenges with the standard contractual clauses include, inter alia, that their terms are inflexible, require the data importer to make its processing facilities available for audit by the data exporter, open all the parties to the potential of liability for non-compliance, and require the execution of clauses with further recipients of the data.

Nevertheless, it is not at all clear that the existing standard contractual clauses are any less susceptible to criticism than the current Safe Harbor Framework. For example, Clause II(c) of the 2004 version of the controller-to-controller clauses (Decision 2004/915/EC) requires a data importer to warrant that "[i]t has no reason to believe, at the time of entering into [the] clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under [the] clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws." How many US companies entering into these clauses have notified the data exporter of the various laws that might require them to disclose personal data transferred to US authorities (whether for anti-terrorism, investigatory, judicial, or any number of other purposes), and how many data exporters have passed this information on to the relevant DPA? Moreover, assuming such a notification were to occur, following the reasoning of the CJEU opinion, it is difficult to see how the DPA could then allow transfers to occur without at least making two determinations with respect to each such law: Namely, that (1) the law limits the collection of personal data to that which is strictly necessary, and (2) either the EU DPA itself or some independent authority in the third country has effective oversight over such collections and can ensure compliance with the "strictly necessary" condition.

Binding corporate rules may well suffer from the same infirmity. Indeed, it could be argued that BCRs are more problematic from the point of view of allowing individuals the opportunity for effective judicial redress because the specific terms of many companies' BCRs are not public. For example, if Facebook had used BCRs to transfer personal data to the US rather than the Safe Harbor Framework, how could Mr. Schrems have been able to determine if his transferred data was adequately safeguarded without being given access to the precise terms of the BCRs used to legitimize the transfer? Moreover, in the event a data subject like Mr. Schrems were to lodge a complaint with a DPA alleging that a data transfer conducted pursuant to the standard contractual clauses or BCRs violated his data protection rights, DPAs would appear obligated to independently assess the adequacy of these safeguards, at least where there is sufficient evidence to suggest a risk that data protection rights are being violated (e.g., the circumstances noted in the Schrems case). In effect, the CJEU seems to have unleashed the potential for numerous Member State DPA investigations of whether jurisdictions deemed "adequate" by the Commission remain "adequate," and inconsistent assessments of whether particular safeguards approved by the Commission or by other data protection authorities as "adequate" are indeed "adequate."

Future of the Safe Harbor Framework

The US Department of Commerce and European Commission have been negotiating a revised Safe Harbor Framework since early 2014. These negotiations followed a report by the European Commission issued in December 2013 concluding that modifications to the Framework were necessary to increase transparency and oversight. These negotiations were first scheduled to conclude in summer 2014, then the deadline for agreement was pushed back to summer 2015. At present, the sides are reportedly very close to an agreement, but nothing final has yet been publicly announced. Assuming the new Framework ("Safe Harbor 2.0") addresses only the 13 recommendations contained in the Commission's 2014 report (available here), it is unclear if that new Framework would actually satisfy the CJEU's findings concerning how "adequacy" must be assessed. Indeed, it is possible that the parties may need to return to the negotiating table to address, for example, the additional recommendations made by the Article 29 Working Party concerning weaknesses in the current Framework (available here).

Moreover, while the US and EU announced last month that agreement has been reached on an "Umbrella Agreement" for the exchange of information for purposes of investigation, detection, and prosecution of criminal offenses, the agreement appears only to apply to direct transfers between EU and US law enforcement agencies. It does not appear to apply to US law enforcement's collection of personal data transferred from the EU to US companies. Finalization of the Umbrella Agreement will not take place until the Judicial Redress Act (HR 1428) is passed into law. The Judicial Redress Act will extend provisions of the US Privacy Act of 1974 to EU citizens. For example, it will give EU citizens the right to access and request correction of information a US federal agency collects on them, subject to certain exceptions, and it provides for judicial remedies if an agency unlawfully discloses personal information about them. The Judicial Redress Act should address some of the concerns raised concerning onward transfers of EU personal data to US government authorities, but it is unlikely to address concerns relating to the gathering of information by US intelligence agencies as there are various exceptions that apply under the Privacy Act with respect to ongoing investigations.

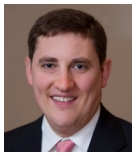
What's Next?

In response to today's decision, it is likely that the US Department of Commerce and European Commission will release further information in the near term as to when Safe Harbor 2.0 is likely to be finalized. We anticipate that EU data protection authorities will quickly issue guidance for companies that have been relying on the Safe Harbor Framework for the transfer of personal data on what other options are available. As a practical matter, it would seem unlikely that DPAs would take immediate action to suspend transfers by companies relying on the Safe Harbor Framework, but individual data subjects could seek a court injunction to stop transfers. The decision may well also impact the ongoing trilogue negotiations among the European Commission, Council, and Parliament concerning a new General Data Protection Regulation (GDPR). The European Parliament has proposed the inclusion of an article that would require an EU data controller or processor to notify the relevant DPA of any request received to disclose personal data as a result of a third country's judgment or decision of a court, tribunal or administrative authority (Article 43a). The controller or processor would have to obtain prior authorization from the DPA for the transfer or disclosure. In addition, the controller or processor would be required to notify the affected individual of the request and, as applicable, of the DPA's authorization. Although the Council has been reluctant to agree to such an article, today's decision is likely to provide momentum to those supporting its inclusion.

A copy of the CJEU decision can be downloaded here.

Privacy & Data Security Team

Primary Contacts



Peter Blenkinsop
Partner
Washington, D.C.
(202) 230-5142
Peter.Blenkinsop@dbr.com

Mary Devlin Capizzi
Partner
Washington, D.C.
(202) 230-5101
Mary.DevlinCapizzi@dbr.com

Stanley W. Crosley
Partner
Washington, D.C.
(317) 770-7399
Stanley.Crosley@dbr.com

Drinker Biddle®
www.drinkerbiddle.com
CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | WASHINGTON DC | WISCONSIN