Bloomberg BNA

Privacy and Security Law Report®

EU-U.S. Privacy Shield

Official Responses and Brexit

There is no guarantee that the EU-U.S. Privacy Shield data transfer program won't be subject to further challenge before the European courts, with dissenting voices continuing to criticize the new deal and uncertainty about how Brexit may impact the situation. Companies would be well advised to consider other methods of legitimizing the transfer of personal data from the European Economic Area to the U.S., or where possible, silo data within the EEA so that cross border data transfer issues don't arise, the authors write.

Concrete Solution, or Are the Sands Still Shifting? European Data Protection Post-*Schrems*

BY EMMA FLETT AND SHANNON YAVORSKY

Emma Flett is an intellectual property partner in Kirkland & Ellis International LLP in London. She can be reached at emma.flett@kirkland.com.

Shannon Yavorsky is an intellectual property partner in Kirkland & Ellis LLP in San Francisco. She can be reached at syavorsky@kirkland.com.

In the months following *Case C-362/14 Maximillian Schrems v Data Protection Commissioner* (*Schrems*) (14 PVLR 1825, 10/12/15), in which the Court of Justice of the European Union (CJEU) invalidated the European Commission's Safe Harbor Decision (2000/520/EC), issues with respect to the transfer of personal data from the European Economic Area (EEA) to the U.S. have continued to evolve, leaving little certainty for companies engaged in cross border data transfer. Post-*Schrems*, personal data can no longer be transferred from the EEA to U.S. companies that self-certified to the Safe Harbor regime without such companies providing an alternative mechanism to adequately protect the data on transfer.

As has been previously reported, national data protection authorities (DPAs), both within and outside the EEA, urged data controllers who were previously relying on Safe Harbor to reconsider the legal basis for transferring data from Europe to the U.S., with some DPAs suggesting that companies should enter into "Model Contract Clauses" in order to legitimize such data transfers. However, Model Contract Clauses were seen by some as a temporary solution (with certain German DPAs rejecting this option entirely), and it was widely recognized that a longer-term, more concrete solution needed to be reached to the problem of transat-

 ISSN 1538-3423

lantic data flows. Following crisis talks between the European Commission and U.S. officials, a deal was announced on Feb. 2, 2016—called the EU-U.S. Privacy Shield—as the proposed solution to this problem (15 PVLR 269, 2/8/16).

The Privacy Shield, in a revised form intended to address criticisms of the February text, was adopted by the Commission on July 12; there is, however, no guarantee that it won't be subject to further challenge before the European courts, with dissenting voices continuing to criticize the new deal. To complicate matters, the Irish DPA recently referred certain questions on the adequacy of the Model Contract Clauses to the Irish Courts for further referral to the CJEU. In short, issues with respect to the transfer of personal data outside the EEA don't appear to be fully settled and the sands, for now, continue to shift.

The EU-U.S. Privacy Shield

On Feb. 29, 2016, the European Commission issued the various texts which form the Privacy Shield, including a series of letters and written commitments from the U.S. Department of Commerce, U.S. Secretary of State, U.S. Secretary of Transportation, U.S. Department of Justice, the Office of the Director of National Intelligence and the Federal Trade Commission.

Like the Safe Harbor regime, the Privacy Shield requires U.S. businesses to sign up to a series of principles, register to be on a compliance list (called the Privacy Shield List), and self-certify that they meet the regime's requirements if they wish to receive personal data from the EEA. The framework will be largely enforced by the U.S. Department of Commerce and the U.S. Federal Trade Commission, as the U.S. government was reluctant to allow this role to be carried out by the EU DPAs themselves. These U.S. authorities will publish a list of companies which have signed up to the Privacy Shield, and those which have been excluded for breaching its terms.

Broadly, the terms of the Privacy Shield impose stronger obligations on U.S. companies to protect the personal data of individuals within the EEA as compared to the Safe Harbor regime. Notably, there are requirements of greater transparency, increased monitoring of compliance and explicit redress mechanisms, including the establishment of an ombudsperson mechanism tasked with handling complaints from individuals. In addition, as a result of concerns voiced by various parties, including the EU's Article 29 Working Party (a body comprised of representatives from the national DPAs of all Member States) (WP29), the final version of the Privacy Shield includes a number of critical amendments designed to address specific concerns about the initial proposal (as further discussed below).

Responses

On Feb. 29, 2016, the same day as the publication of the texts which form the substance of the Privacy Shield, the European Commission also published a draft ''adequacy decision'' which states that, following these commitments, the U.S. can be seen as providing an adequate level of protection of personal data—i.e., equivalent to the protections offered by EU law (15 PVLR 462, 3/7/16). However, this did not mark the agreement as a done deal. Both the WP29 and the European Data Protection Supervisor (EDPS) raised objections to the Privacy Shield as then drafted. In *Schrems*, the Safe Harbor regime was severely criticized by the CJEU for failing to prevent U.S. authorities (such as the National Security Agency) from collecting EU citizens' data in bulk. Several parties, including the WP29 and the EDPS have separately criticized the Privacy Shield (as it was presented in February) as not adequately remedying this problem. The WP29 and the EDPS explicitly stated that the February draft of the Privacy Shield failed to ensure protection ''essentially equivalent'' to EU law.

The Article 29 Working Party was concerned specifically that the February draft of the Privacy Shield did not adequately prevent the U.S. authorities from collecting European Union citizens' personal data indiscriminately and in bulk.

WP29

The WP29 issued its *Opinion 01/2016 on the Privacy Shield draft adequacy decision* on April 13, 2016, in which it stated that certain ''key data protection principles as outlined in European law are not reflected in the [Commission's] draft adequacy decision and the annexes, or have been inadequately substituted by alternative notions'' (15 PVLR 825, 4/18/16)

The WP29 was concerned specifically that the February draft of the Privacy Shield did not adequately prevent the U.S. authorities from collecting EU citizens' personal data indiscriminately and in bulk. The text of the Privacy Shield allowed U.S. authorities to collect such data in bulk for the purposes of ''detecting and countering certain activities of foreign powers; counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to U.S. or allied armed forces; and combating transnational criminal threats, including sanctions evasion''. The WP29 believed that such broad possible derogations to the principles of data privacy ''do not exclude massive and indiscriminate collection of personal data originating from the EU.'' Such criticisms have been voiced by many, notably including Max Schrems himself, who said that ''Basically the U.S. openly confirms that it violates EU fundamental rights in at least six cases. . . .'' The WP29 also made it very clear that ''massive and indiscriminate surveillance of individuals can never be considered as proportionate and strictly necessary in a democratic society.''

EDPS

As previously reported, the EDPS, Giovanni Buttarelli, published *Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision* on 30 May 2016 (15 PVLR 1161, 6/6/16). Buttarelli praised the Privacy Shield as a genuine attempt to improve upon the Safe Harbor regime, noted that several improvements were apparent, and acknowledged the involvement of several

   ISSN 1538-3423

key U.S. governmental organisations, particularly the Department of State, the Department of Justice, and the Office of the Director of National Intelligence. However, he also made it clear that the Privacy Shield, as drafted in February, would suffer a similar fate to Safe Harbor unless ''significant improvements'' were made, and that ''progress compared to the earlier Safe Harbour Decision is not in itself sufficient. The correct benchmark is not a previously invalidated decision. . . .''

The EDPS echoed the concerns of the WP29 regarding the bulk collection of European citizens' data by U.S. authorities and felt that the February draft of the Privacy Shield would likely be seen as legitimizing such mass collection. Furthermore, the EDPS was critical of the agreement's lack of provisions concerning data retention.

European Parliament

In May, the European Parliament noted that the Privacy Shield contained ''substantial improvements'' as compared to Safe Harbor, but that it still contained a number of ''deficiencies.'' According to the European Parliament, U.S. authorities would still have unacceptably broad access to the personal data of EU citizens. It also echoed the criticisms of others regarding the apparent lack of independence of the new ombudsperson, which would not be ''vested with adequate powers to effectively exercise and enforce its duty,'' and the proposed redress mechanism which was described as overly complex and needed to be more ''user-friendly and effective.''

U.K.

On Feb. 11, 2016, the U.K.'s national DPA, the Information Commissioner's Office (ICO) published a blog post stating that ''it is too early to say whether the new Shield provides adequate protection for personal data passed from the EU to the USA.'' However, the ICO also said that it ''will not be seeking to expedite complaints about Safe Harbor while the process to finalise its replacement remains ongoing and businesses await the outcome.''

At the Westminster eForum on April 28, 2016, U.K. Information Commissioner Christopher Graham urged U.S. companies to put pressure on U.S. government officials to answer the ''simple, relevant questions'' raised of the Privacy Shield by the WP29. ''You can be sure that the European Court of Justice would also be asking these questions,'' Graham said, clearly referring to the possibility that the highest court in Europe may invalidate the Privacy Shield if it is not convinced that this agreement genuinely secures an ''adequate'' standard of protection for personal data which is sent to the U.S. from the EEA.

Amendments to the Privacy Shield

In light of such strong concerns over deficiencies contained in the February draft of the Privacy Shield, negotiations were resumed between the EU and the U.S. In June 2016, a revised agreement was reached which remedied many of these concerns. The White House has confirmed in writing that bulk collection of data will be ''as targeted and focused'' as possible. The Privacy Shield now explicitly contains rules on data retention, so U.S. companies will be required to delete data they hold which becomes redundant for the purpose for which it was collected. Furthermore, in order to address concerns about the impartiality of the new ombudsperson, the U.S. has agreed that this body will be independent from national security services.

Is the Privacy Shield Now Set in Stone?

On 25 June 2016, the European Commission submitted the revised draft of the Privacy Shield adequacy decision to the Article 31 Committee, a group of representatives of the Member States. The Privacy Shield was formally adopted by the Commission on 12 July 2016, and companies will be able to certify with the U.S. Department of Commerce starting 1 August 2016. However whilst it may appear that the sands are beginning to settle, companies should keep developments under close review, as privacy advocates have already suggested that the Privacy Shield may be challenged before the CJEU, notwithstanding the Commission's declaration that the revised and adopted version reflects the court's requirements.

Fines and Enforcement Post-*Schrems*

In the months following the *Schrems* decision, most national DPAs have taken a hesitant approach to enforcement against U.S. companies which continue to transfer data from the EEA to the U.S. on the sole basis of Safe Harbor. Indeed, the U.K. ICO stated that it will be ''sticking to [its] published enforcement criteria and not taking hurried action whilst there's so much uncertainty around and solutions are still possible.'' However, a German DPA took a different view and has fined Unilever PLC, Adobe Systems Inc., and Punica Getranke GmbH (15 PVLR 1227, 6/13/16) (although admittedly fairly small sums) for transferring personal data to the U.S. from Europe and relying only on Safe Harbor post-*Schrems*.

The U.K. would presumably not wish to significantly diverge from the General Data Protection Regulation for fear of being deemed ''not adequate'' by the European data protection authorities.

Impact of Brexit

On June 23, 2016, the U.K. public voted, by a 52 percent majority, to leave the EU. It is still very unclear whether, and/or on what terms, this will happen. However, assuming the U.K. does in fact leave the EU, the U.K. will no longer be bound by EU data protection law or covered by the Privacy Shield, nor will it be bound by the obligations of the EU General Data Protection Regulation (GDPR) (unless it remains a member of the EEA). There is likely to be a period of cross-over between the coming into force of the GDPR (25 May 2018) and the U.K.'s departure from the EU; although it is un-

certain whether the U.K. government will honour its obligations under the GDPR during this period.

The ICO said in an official statement on 19 April 2016 that ''the U.K. will continue to need clear and effective data protection laws, whether or not the country remains part of the EU.'' Furthermore, if the U.K. leaves the EU, the U.K.'s data protection regime will still need to be recognized by the European Commission as ''adequate'' (i.e. providing an equivalent standard of protection as is afforded in the EU) in order for personal data to be freely transferred from the EU to the U.K. post-Brexit.

The possible future invalidity of Model Contract Clauses as a means of lawful data transfer to the U.S. may well have influenced the Article 31 Committee's decision to approve the EU-U.S. Privacy Shield as an alternative.

It seems highly likely that a failure to comply with at least the spirit of the GDPR would be fatal to such an adequacy decision; thus the U.K. would presumably not wish to significantly diverge from the GDPR for fear of being deemed ''not adequate'' by the European data protection authorities. However, whether the U.K. will retain the provisions of the GDPR verbatim remains to be seen. Indeed, if the data protection laws adopted by the U.K. are not deemed adequate by the European Commission, it is also not out-of-the-question that the Privacy Shield or a similar regime may be put in place between the U.K. and the EU to provide adequacy to personal data on transfer.

It has been suggested in commentary, albeit speculatively, that the CJEU may be less inclined to invalidate the Privacy Shield as a means of legitimizing transatlantic data transfer than it was in respect of Safe Harbor. Given the already considerable degree of legal uncertainty in Europe surrounding Brexit, the CJEU may not wish to add to this by rejecting an attempted solution to the question of data flows from Europe to the U.S.

Model Contract Clauses Called Into Question

On May 25, 2016, the Irish Data Protection Commissioner stated that it will refer the legality of personal data transfers under the Model Contract Clauses to the Irish High Court for declaratory relief, with the intention of this question being further referred to the CJEU. It has been suggested that the CJEU may hold these clauses invalid for much the same reason as it did for Safe Harbor in *Schrems*, namely that the Model Contract Clauses fail to prevent the wholesale collection of European citizens' personal data by U.S. authorities.

As the Privacy Shield has now been approved by the Article 31 Committee and will shortly come into effect, this issue will likely be avoided. Indeed, the possible future invalidity of Model Contract Clauses as a means of lawful data transfer to the U.S. may well have influenced the Article 31 Committee's decision to approve the Privacy Shield as an alternative; although global companies such as Facebook Inc.—Facebook has been involved in numerous legal battles relating to data protection, including the *Schrems* case—will likely be following the Irish High Court case, and possible future CJEU referral, carefully.

Conclusion

The months of uncertainty surrounding European data protection and EU-U.S. data flows seem to be slowly settling; though given ongoing criticism of the various methods of cross border data transfer, companies should continue to closely monitor this landscape. This new agreement will allow certified U.S. companies once again to lawfully transfer personal data from the EEA to the U.S. without having to rely on Model Contract Clauses, the legality of which is currently being challenged, or face fines and other enforcement action by the various European DPAs.

As to Brexit, if the U.K. does leave the EU, it will not be legally bound to keep its national laws in conformity with the obligations contained in the GDPR (unless it remains part of the EEA); however it seems highly likely that the U.K. would choose to do so, due to the fear of its data protection laws being deemed not to offer ''adequate'' protection as compared to EU law. The Privacy Shield may offer a concrete solution to cross border data transfer but given ongoing scrutiny, companies would be well advised to also consider other methods of legitimizing the transfer of personal data from the EEA to the U.S., or where possible, silo data within the EEA so that cross border data transfer issues do not arise.

  PVLR ISSN 1538-3423