Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 11 >>> NOVEMBER 2015

Responses from Inside and Outside the EEA to the ECJ's Ruling on Safe Harbor: Shifting Sands

By Shannon Yavorsky, in the San Francisco office, and Emma L. Flett, in the London office, of Kirkland & Ellis LLP.

As has been widely reported, on October 6, 2015, the European Court of Justice (ECJ) handed down its landmark ruling in *Maximillian Schrems v Data Protection Commissioner* ("*Schrems*") (Case C-362/14). In *Schrems*, the ECJ held that the European Commission's Safe Harbor Decision (2000/520/EC) — in which the Commission found that an adequate level of protection is ensured when personal data is transferred to Safe Harbor-certified companies — was invalid. Specifically, the ECJ found that the U.S.-EU Safe Harbor Program does not provide an adequate level of protection because, amongst other things: 1) it is unable to protect EU personal data from access by U.S. intelligence agencies and is subject to derogations implemented by U.S. legislation, and 2) it is essential to the fundamental right to privacy that a data subject has a right of recourse to the applicable national data protection authority (DPA) to hear a citizen's data protection concerns (*see analysis at WDPR, October 2015, page 4*).

This means that, as of October 6, 2015, transfers of personal data from the European Economic Area (EEA) — the 28 EU member states plus Iceland, Liechtenstein and Norway — to the U.S. can no longer be based on the invalidated Safe Harbor decision, and companies should consider alternative solutions for cross-border data transfers.

However, the range of responses which have followed *Schrems*, on a near daily basis, as to what steps to take on a practical level, have not been so easy to follow. Nor has it been easy to assess whether the option of sitting tight while the EU and the U.S. resolve their differences over a strengthened data transfer framework is a viable one.

Several national DPAs (both within and outside the EEA), the EU Article 29 Data Protection Working Party (an advisory body made up of representatives from the DPA of each E.U. member state, the European Data Protection Supervisor and the European Commission) and the European Commission have weighed in on what methods remain available to legitimise the transfer of data outside the EEA. There are conflicting views, and what may be accepted by one DPA may not be permitted by another. As a result, organisations need to carefully consider each data flow, including the jurisdiction from which the data is being transferred, to consider the most appropriate mechanism to legitimise the transfer. It may be that a combination of methods should be employed, depending on the nature and volume of the data and the relevant jurisdiction, to better comply with applicable national law.

With national data protection authorities continuing to weigh in on the practical implications of the ECJ's ruling, the sands continue to shift. However, the message from most DPAs — with Germany being a notable exception — seems to be that Model Contract Clauses, Binding Corporate Rules and derogations remain viable mechanisms by which to transfer data to the U.S.

We have followed the various responses flowing from *Schrems*, and how the sands have been shifting as a result. We set out below a summary of the views taken by a selection of key data protection regulators, to assist in navigating the post-*Schrems* storm.

Responses from Within the EEA

European Commission

On November 6, 2015, the European Commission published a communication on the "Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)" (Communication) aimed at providing an overview of the alternative tools for transatlantic data transfer under the EU Data Protection Directive (95/46/EC) (Directive) in the absence of an adequacy decision.

The Communication recognises the impact of *Schrems* on transatlantic trade, noting that "the EU and the United States are each other's most important trading partners, and data transfers, increasingly, form an integral part of their commercial exchanges". As to *Schrems*, the Communication observes that the ECJ confirmed that, even where there is an adequacy decision, EU member state DPAs "remain empowered and obliged to examine, with complete independence, whether data transfers to a third country comply with the requirements laid down by the Directive 95/46/EC". However, the Communication points out that the ECJ also found that only the ECJ can declare a Commission adequacy decision invalid.

The Communication notes that concerns have been expressed by industry as to the possibilities for continued data transfer in the wake of *Schrems*.

With respect to Model Contract Clauses, the Communication states that, since Commission decisions are binding in their entirety on EU member states, using the Model Contract Clauses means that DPAs are, in principle, under the obligation to accept those clauses, and, as a result, may not refuse the transfer of data solely on the basis that the Model Contract Clauses do not offer sufficient safeguards. However, the Commission recognises that this is without prejudice to the DPAs' power to examine the clauses in light of *Schrems*. The Commission states that, if a DPA has doubts about the compatibility of the Model Contract Clauses with the Directive, it should refer the question to its national court, which can in turn refer the question to the ECJ.

As to other methods of cross-border data transfer, the Communication further states that Binding Corporate Rules (BCRs) and the derogations under Article 25(6) of the Directive still apply, although, as the Commission acknowledges by echoing earlier guidance of the EU Article 29 Working Party, the derogations are of limited application to transfers of personal data characterised as "repeated, mass or structural".

Overall, the Communication seeks to calm the waters roiled by conflicting information coming out of local DPAs, and goes some way towards achieving that goal by confirming the legal position with respect to the Model Contract Clauses, BCRs and the derogations.

EU Article 29 Working Party

The Article 29 Working Party issued a statement on October 16, 2015, noting that transfers that are still taking place under the Safe Harbor after *Schrems* are unlawful.

The Working Party confirmed that it is analysing the impact of *Schrems* on transfer tools, and considers that Model Contract Clauses and BCRs can still be used whilst the analysis is ongoing. It notes, "Businesses should reflect on the eventual risks they take when transferring data and should consider putting in place any legal and technical solutions in a timely manner to mitigate those risks". However, the Working Party notes that this will not prevent DPAs from investigating particular cases. The statement says that current negotiations with respect to a new Safe Harbor could form part of the solution. Further, the statement notes that if, by the end of January 2016, no appropriate solution is found with U.S. authorities, EU data protection authorities are committed to take "all necessary and appropriate actions", which may include "coordinated enforcement actions".

Germany

The German DPAs — consisting of the data protection commissioners of the federal states and the federal data protection commissioner — issued a joint position paper on October 26, 2015, calling into question the lawfulness of data transfers to the U.S. based on Model Contract Clauses and BCRs (*see report in this issue*).

Further, the position paper indicates that the German DPAs will prohibit data transfers to the U.S. that are based solely on Safe Harbor, and will not issue new approvals for data transfers to the U.S. on the basis of Model Contract Clauses or BCRs. However, the position paper specifies that "consent for the transfer of personal data can be a sound basis if subject to restrictive conditions. In principle, the data transfer must not occur repeatedly, in mass quantities or routinely". Consistent with the position taken by other DPAs, the position paper also notes that "consent can only in exceptional cases be a permissible basis for data transfers to the USA if the export concerns personal data of employees or if

   ISSN 1473-3579

data of third persons are affected at the same time". The German DPAs also indicate their view that the Model Contract Clauses will have to be adjusted to the requirements of *Schrems*, but do not provide any further color in this regard, commenting only that they welcome the deadline of January 31, 2016, set by the Article 29 Working Party.

U.K.

The Information Commissioner's Office (ICO) is the national DPA in the U.K., which regulates both individuals and companies, and provides tools and "best practice" guidance to enable individuals and companies to understand their obligations under the U.K. Data Protection Act 1998.

Following *Schrems*, the ICO published a blog post on October 27, 2015, setting out its reaction to the decision and its opinion on what companies and individuals should be doing (and should not be doing) as a consequence.

The ICO began by explaining that the ECJ did not "strike down" the Safe Harbor framework itself, but that the ECJ's judgment merely meant that the Commission's Safe Harbor Decision could no longer be relied upon. This means that, in theory, national DPAs can review data transfers purportedly made under the Safe Harbor and decide whether such data is adequately protected, notwithstanding the fact that the recipient may be registered as a Safe Harbor entity. In practical terms, however, DPAs cannot now make such a finding on the basis of Safe Harbor certification alone.

The ICO has summarised its advice to individuals and companies by focusing on three key points:

'Don't Panic'

The ICO recommends that businesses do not rush to put in place alternative transfer mechanisms which may present their own problems. It does, however, stress that the impact of the *Schrems* judgment on Model Contract Clauses and BCRs has yet to be analysed, and, whilst transfers can always be made on the basis of an individual's consent, "this does not protect personal data any more effectively than Safe Harbor. Indeed, individuals may be easily induced to give their consent to the transfer of their data to destinations where there is little or no protection when the Safe Harbor does at least provide them with some genuine protection even if such protection is imperfect".

'Take Stock'

A party which is intending to transfer personal data to another jurisdiction should assess what personal data it is transferring outside the EEA, where is it going, and what arrangements have been made to ensure that the personal data is adequately protected. The business should then consider what transfer mechanism is the most appropriate in the circumstances (*e.g.*, BCRs, consent or Model Contract Clauses). Again the ICO stresses that businesses should not rush to put in place an alternative transfer mechanism, particularly as a new and improved Safe Harbor 2.0 may emerge in the not-too-distant future.

'Make Your Own Mind Up'

The ICO stresses that parties in the U.K. which intend to transfer data abroad are able to make their own adequacy assessments (and indeed has issued separate guidance on how to assess adequacy prior to making a transfer). For data to be adequately protected, much depends on the specifics of the particular transfer. The ICO invites these parties to assess how risks can be mitigated, placing more emphasis on companies doing their due diligence than blindly relying on prescribed contractual clauses.

ICO Enforcement Powers

The ICO has the power to take enforcement action against those it believes have not complied with U.K. data protection legislation. Penalties can include criminal prosecution for serious breaches, non-criminal enforcement audits to check organisations are complying and monetary penalties of up to 500,000 pounds (U.S.$763,620).

The ICO has stated that it will not be rushing to use its enforcement powers, as it does not consider there to be a "new and immediate threat" to individuals' data as a result of the ruling in *Schrems*:

> Of course we'll consider complaints from affected individuals, whatever transfer mechanism you're relying on, but we'll be sticking to our published enforcement criteria and not taking hurried action whilst there's so much uncertainty around and solutions are still possible. We can't create legal certainty where there is none but we will continue to work with our European counterparts in an effort to ensure that, as far as possible, we're all delivering a single and sensible message. Ultimately, for the ICO it has to be a message that is consistent with UK law, with our powers and with the public commitments we have made about when and how we will use those powers.

The ICO has confirmed that it will update its guidance on international transfers in time, but will still deem the majority of previously issued guidance to remain valid.

Responses from Outside the EEA

Responses to *Schrems* have not been confined to just regulators located within the EEA. The ripple effect of this landmark ruling has been felt farther afield, sparking reaction in jurisdictions such as Switzerland, Israel and Dubai.

Switzerland

On October 22, 2015, the Swiss DPA announced that the U.S.-Swiss Safe Harbor is no longer valid for the same reasons set out in *Schrems*.

The Swiss DPA said that additional measures need to be taken in order to meet the requirements of the cross-border data transfer provisions in Swiss data protection legislation. In most cases, the Swiss DPA indicated that

these measures would take the form of Model Contract Clauses or BCRs, and that these measures should be implemented by the end of January 2016 (*see report in this issue*).

In light of the unsettled landscape, companies that transfer data outside the EEA should carefully consider each data flow, paying particular attention to the country from which the data originates and the nature and volume of the data at issue, to determine the most appropriate method or methods to legitimise the transfer.

Israel

On October 19, 2015, the Israeli Law, Information and Technology Authority (ILITA) made an announcement revoking its prior authorization which legitimised data transfers between Israel and Safe-Harbored U.S. companies (*see report in this issue*).

Notably this will hinder data flows to the U.S. from Israel's thriving technology hub comprising R&D and manufacturing plants of global players such as Facebook and Google. Limor Shmerling, the ILITA's director of licensing and inspection, has said that the ILITA is "considering the implications of the new legal status and will further address the subject accordingly". In 2011, the European Commission recognised Israel as a country with "adequacy" status, and personal data has been allowed to flow freely between Israeli borders and EEA countries since this date. As part of Israel's data protection regime, it, like its EEA counterparts, has restricted the movement of personal data to third countries without first putting protective measures in place, including, until now, the U.S. Safe Harbor regime. The Israeli reaction is further evidence of the ripple effect.

Of course, the fact that the ECJ has essentially stated that any European Commission adequacy finding can now be called into question (and not just the adequacy finding relating to Safe Harbor), including that which awarded such status to Israel, adds a further layer of interest. However, as Israel's adequacy status has not been challenged, some have commented that the country could utilise this as a competitive advantage over the U.S. technology sector.

Dubai

Guidance issued by the Dubai International Financial Centre Data Protection Commissioner issued on October 26, 2015, provides a further example of a non-EEA data protection regulator issuing a statement on *Schrems*. This recommends that data controllers who have previously relied on Safe Harbor when transferring personal data to the U.S. review and reconsider the legal basis for transfer.

Conclusion

With national DPAs continuing to weigh in on data transfer, the sands continue to shift. However, the message from most DPAs — with Germany being a notable exception — seems to be that the Model Contract Clauses, BCRs and derogations remain viable mechanisms by which to transfer data to the U.S.

In the meantime, the European Commission indicated in early November 2015 that it is committed to agreeing a new data sharing agreement with the U.S. within three months. For some, this seems optimistic, but with at least one stumbling block out of the way, namely the protracted negotiations over the EU-U.S. data protection "umbrella agreement" on law enforcement co-operation (*see WDPR, September 2015, page 36*), the path to Safe Harbor 2.0 is clearer than it was back in 2013, when the Commission issued recommendations designed to strengthen trust in the original framework.

Speaking at the Amsterdam Privacy Conference on October 23, 2015, U.S. Federal Trade Commissioner Julie Brill also spoke positively of the need "to create a new data transfer mechanism that strengthens the privacy protections that were in the Safe Harbor principles". As to progress towards reaching a new agreement, she said, "Although the text being negotiated by the Commission and the United States has not been made public, I have every reason to believe that both sides understand the need to ensure that these substantive protections are more robust, and that both sides have been working to that end".

In light of the unsettled landscape, however, companies that transfer data outside the EEA should carefully consider each data flow, paying particular attention to the country from which the data originates and the nature and volume of the data at issue, to determine the most appropriate method or methods to legitimise the transfer.

Given how rapidly the terrain is evolving, it remains critical to keep on top of developments in this area, particularly in advance of the deadline for compliance of January 31, 2016, proposed by the EU Article 29 Working Party.

So for now, the message is, don't panic, watch this space and, wherever you may be, keep listening to what your DPA is saying. Meanwhile all, except perhaps EU data processors with commercial interests in the void left by Safe Harbor's demise, will share U.S. FTC Commissioner Brill's hope that EU-U.S. negotiations "come to a speedy and successful conclusion".

The ECJ's decision in Case C-362/14, Maximillian Schrems v Data Protection Commissioner, is available at http://bit.ly/1JSABLP.

The European Commission's communication on the "Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362-/14 (Schrems)" is available at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf.

   ISSN 1473-3579

The EU Article 29 Working Party's statement is available at http://www.cnil.fr/fileadmin/documents/Communications/20151016_wp29_statement_on_schrems_judgement.pdf.

The German data protection commissioners' joint position paper is available, in German, at https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/EuGH_erkl__rt_Safe_Harbor_f__r_ung__ltig_-_UPDATE/DSK_Positionspapier_151026.pdf.

The U.K. ICO's blog post is available at https://iconewsblog.wordpress.com/2015/10/27/the-us-safe-harbor-breached-but-perhaps-not-destroyed/.

The Swiss DPA's announcement is available, in French, at http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=fr.

The Israeli Law, Information and Technology Authority's announcement is available, in an unofficial English translation, at https://iapp.org/media/pdf/resource_center/ILITA_SH_Statement.pdf.

The Dubai International Financial Centre Data Protection Commissioner's guidance is available at http://www.difc.ae/sites/default/files/DIFC-Data-Protection-Commissioner-Guidance-on-Adequacy-Status-relating-to-US-Safe-Harbor-Recipients.pdf.

Shannon Yavorsky is a Partner in the San Francisco office and Emma L. Flett is a Partner in the London office of Kirkland & Ellis LLP. They may be contacted at shannon.yavorsky@kirkland.com and emma.flett@kirkland.com.