Client ALERT

WOMBLE CARLYLE

Bond Dickinson | WOMBLE CARLYLE

A TRANSATLANTIC LAW FIRM ALLIANCE FOR BUSINESS

A Fragile Shield? Managing the Risks of EU-U.S. Data Transfer

July 26, 2016

On July 12, 2016, the European Commission formally adopted "Privacy Shield" to govern EU-U.S. personal data transfers and to provide EU data subjects with meaningful recourse should they have grounds to complain about the handling of their data.

Privacy Shield was negotiated as an urgent replacement for the Safe Harbor regime, which was struck down by the European Court of Justice (ECJ) in October 2015 following a challenge by privacy campaigner Max Schrems. Although formally adopted, Privacy Shield is itself likely to face challenge from Schrems and others who consider it an inadequate response to the ECJ's objections. Meanwhile, EU Standard Contractual Clauses (the "Model Clauses") – which are another mechanism by which personal data can be lawfully exported outside the EU – are also on their way to the ECJ following a referral decision by the Irish data protection regulator. This combined uncertainty means that organizations must consider contingency plans and fall-back positions to ensure that personal data transfers from the EU to the U.S. remain lawful and uninterrupted.

On both sides of the Atlantic, ensuring that personal data can lawfully flow as part of business-critical processes requires close monitoring and well-advised responses to a rapidly evolving situation. Our Privacy and Data Protection Team experts have been discussing the issues with their counterparts in our UK strategic partner firm Bond Dickinson to highlight areas where specific advice and collaborative thinking will be needed. Here are their thoughts.

What Are the Key Practical Issues?

- Should U.S. organizations self-certify for Privacy Shield?
- If so, when?
- Should self-certification for Privacy Shield replace or be an additional measure to the use of Model Clauses?
- What steps should EU organizations take to protect themselves against a successful challenge, whether to Privacy Shield or the Model Clauses?

- What can we say, at this stage, about the "Brexit effect"?

Is Privacy Shield Vulnerable to Challenge?

Privacy Shield is likely to be challenged. The European Commission's decision addressed a number of points raised in the ECJ's *Schrems* judgment, including intelligence safeguards regarding bulk collection of data and the creation of a new U.S. Government Ombudsperson with whom data subjects can file complaints about data accessed or used for national security purposes. However, Max Schrems and other EU privacy campaigners remain unconvinced that Privacy Shield adequately protects the privacy of personal data transferred from the EU to the U.S.

There are other potential issues with the Privacy Shield. The Privacy Shield is founded on commitments given by the current U.S. administration; it remains to be seen whether a change in administration in January 2017 would have any impact on those commitments, although the Privacy Shield, and the greater certainty it may bring to businesses for personal data transfers, has enjoyed broad support within the U.S. business community, including the U.S. Chamber of Commerce and other business groups. The Privacy Shield will also need review prior to the application of the new European General Data Protection Regulation in May 2018 and amendments or further challenges may arise as a result.

The real risk of renewed legal challenge is undoubtedly a factor when considering whether, or when, to incur the compliance costs related to Privacy Shield. Self-certification is due to open on August 1, 2016, but in our view it would be prudent (at least for the time being) to keep Model Clauses in place even if self-certifying because of the foreseeable risk of a challenge to Privacy Shield. There are still advantages to self-certifying (even if an organization maintains its Model Clauses). For instance, being a member of Privacy Shield makes it easier to receive personal data from another Privacy Shield member and the Privacy Shield certification will undoubtedly signal an organization's commitment to privacy (even if the scheme itself is challenged).

For U.S. organizations, there may be an incentive to self-certify early where personal data is likely to be transferred to third parties, including sub-processors. Organizations that self-certify within two months after August 1, 2016 will have the benefit of a nine month grace period to bring their pre-existing third party commercial relationships into compliance with the Onward Transfer Principle. Whether that grace period is a sufficient incentive for early registration depends, in part, on the balance between:

- The financial and time costs of self-certification,
- The commercial benefits of early certification, and
- The possibility that Privacy Shield will prove to be as vulnerable as Safe Harbor to a legal challenge in the EU.

As a practical matter, U.S. organizations might reasonably conclude that self-certification under the Privacy Shield makes sense as an addition to, but not as a complete and immediate replacement for, the use of Model Clauses. The outcome of the Model Clauses referral to the ECJ is unlikely to be known for another 18-24 months, and in the interim their continued use might at least temporarily be a more straightforward and a cost-effective basis for EU-U.S. personal data transfers than rushing to self-certification. However, should the Model Clauses be struck down, then it would be strongly in the interests of U.S. organizations already to have gone through, or to be sufficiently advanced in the process of self-certification, to minimize the risk of business interruption.

For EU organizations with no control over the outcome of the ECJ challenges there are practical measures that can be taken. Organizations could choose to avoid transferring personal data to the U.S. (although in some circumstances this may not be feasible). Alternatively, EU organizations can protect themselves by ensuring that they have in place contractual provisions allowing them to:

- Review, and if necessary amend, the terms of the transfer of personal data should challenges to either the Privacy Shield or the Model Clauses succeed, or

- Terminate data transfer arrangements relying on those transfer mechanisms if successfully challenged, and seek a viable replacement.

However, it may be difficult in practice to obtain those contractual commitments (for example, when dealing with large public cloud providers).

Assessing the Cost: What are the Key Differences Between Safe Harbor and Privacy Shield?

Any organization considering self-certification under Privacy Shield must be fully aware of the points at which Privacy Shield follows or differs from Safe Harbor.

Like Safe Harbor, Privacy Shield is based on self-certification by U.S. organizations. Self-certification carries a commitment to comply with the Privacy Shield Principles, but Privacy Shield has significantly strengthened the Safe Harbor principles. For example:

- **Notice:** privacy policies must be made public, and must (if online) contain hyperlinks to the Department of Commerce's website and Privacy Shield list of self-certified companies, along with details of the recourse mechanisms available for data subjects.

- **Security and Onward Transfer:** U.S. organizations must have a written contract with onward recipients of personal data guaranteeing the same level of protection as provided by the Principles and must take steps to ensure its proper implementation.

- **Recourse Mechanisms:** The U.S. organization must put in place an effective recourse mechanism to deal with a complaint received from an EU data subject. Data subjects can now bring a complaint of non-compliance:

    - Directly to the U.S. organization concerned;

    - To an independent dispute resolution body designated by the U.S. organization to resolve such complaints; or

    - To a national data protection authority, the U.S. Department of Commerce, or the U.S. Federal Trade Commission (FTC).

There is also a final recourse available to data subjects of binding arbitration by a "Privacy Shield Panel".

Further key new requirements under the Privacy Shield are discussed in our July 12, 2016 Client Alert about the Privacy Shield..

Assessing the Cost: What is the Process for Self-Certifying Under Privacy Shield?

To join Privacy Shield, a U.S. organization must:

- Self-certify annually its agreement to the Privacy Shield Principles. This self-certification is enforceable under U.S. law by either the FTC or the U.S. Department of Transportation (**DOT**). Any organization subject to either FTC or DOT jurisdiction is eligible to self-certify.

- Identify the independent recourse mechanism it will make available to EU data subjects.

- Develop a Privacy Shield-compliant Privacy Policy Statement that is publicly available and effective *before* self-certification.

- Create a program to verify compliance, either by self-assessment tools or by third party assessment.

- Designate an organizational Privacy Shield contact person, whether the corporate officer certifying compliance or another representative, such as the Chief Privacy Officer.

Clearly, taking those steps requires considerable commitment of time and employee resources, and also requires board or senior-level engagement to ensure that policies and procedures are both formally adopted and have sufficient buy-in and management backing to ensure consistent and successful implementation in practice. In particular, U.S. organizations must decide whether to design and implement an internal verification program or to outsource that function to third party consultants.

Organizations electing to design their own program will have to factor in the opportunity cost in terms of management and other key personnel time/resource to ensure that the program is designed and implemented as efficiently as possible. For organizations that opt for third party verification, there is likely to be something of a race, and could perhaps be a bit of a price war, as suitably qualified and experienced experts are snapped up by eager corporate clients.

The Brexit Effect?

Of course, the impact of Brexit must also be considered. On June 23, 2016, the UK voted to leave the European Union. The precise terms and timing of that withdrawal will determine what steps, if any, need to be taken to replace or replicate Privacy Shield.

It is possible that UK withdrawal from the EU might involve signing up to an alternative basis for access to the single market – for example, joining the European Economic Area (EEA). As a condition of EEA membership, the UK might be required to accept obligations (such as free movement of labor, capital and goods), but as a result might be entitled to benefit from the EU's international agreements, including Privacy Shield.

UK withdrawal from the EU could, alternatively, be far more substantial and complete. The mechanism for UK withdrawal would be implementation of Article 50 of the Lisbon Treaty. Once triggered, Article 50 begins a two year process within which the EU and the departing State might negotiate terms to moderate the impact of withdrawal. However, if no agreement is in place before the final withdrawal date then EU Treaties and laws cease to apply to, or to benefit, the departing State. In that case, the UK would have to consider how best to preserve the benefit of mechanisms such as Privacy Shield.

At its simplest, the UK response might be to recognize Privacy Shield as a mechanism providing adequate protection to data subjects, on the basis that if it is good enough for EU data subjects then it must also be good enough for those in the UK. However, there may be a need for an additional layer of direct agreement between the UK and U.S. to ensure that the recourse and enforcement mechanisms provided under Privacy Shield are equally available to UK data subjects; Privacy Shield would need to be amended as by its terms, it only covers transfers of personal data from the EU and the current EEA member states (Iceland, Liechtenstein and Norway).

Brexit is already proving to be an extremely complex, and probably a protracted, process. Given the business-critical importance of lawful and uninterrupted data flows between the UK and U.S., it will be an issue requiring close attention and ongoing discussion between our data law experts.

Please click on the following links to access the full version of the adequacy decision along with the corresponding annexes.

Contact Information

If you have any questions about this client alert please contact Doug Bonner at 202.857.4428 or DBonner@wcsr.com or Andrew Kimble at +44 (0) 238.020.8422 or Andrew.Kimble@bonddickinson.com.

_____