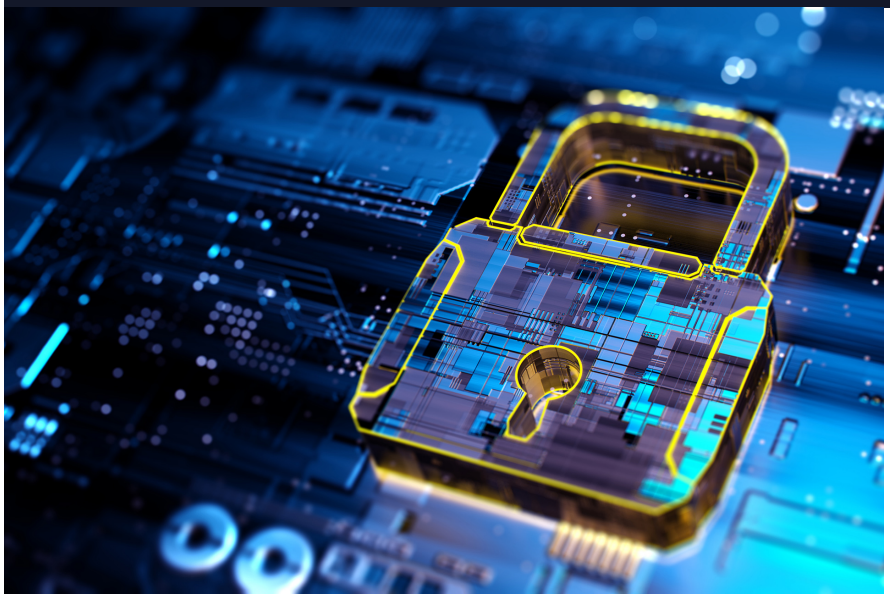
BARNES & THORNBURG LLP



ALERTS

Data Security And Privacy And Compliance Alert - EU-U.S. Privacy Shield Set To Replace Safe Harbor: Smooth Sailing Or Rough Waters Ahead?

March 3, 2016 | Atlanta | Chicago | Columbus | Dallas | Delaware | Elkhart | Fort Wayne | Grand Rapids | Indianapolis | Los Angeles | Minneapolis | South Bend

Officials in the European Union (EU) and United States have been scrambling to replace the U.S.-EU Safe Harbor – the data privacy accord – for the past four months. Now, more details have emerged about the new tentative agreement, dubbed the EU-U.S. Privacy Shield, and they are shaking things up. Any American company doing or considering doing business in Europe or collecting data from European citizens must now assess whether and how to legally comply with requirements relating to the transfer of data from the EU to the U.S. in this unsettled interim. Unfortunately, the answers are far from clear.

The U.S.-EU Safe Harbor previously provided a mechanism for companies to legally transfer personal information collected in Europe about European citizens to the U.S. while certifying that the information would be protected at the highest levels required by the EU's Data Protection Directive. As covered in a previous alert, the Safe Harbor was invalidated as a means of legal transfer following the European Court of Justice's Oct. 6, 2015, ruling in *Maximillian Schrems v Data Protection Commissioner*.

Efforts to update and replace the Safe Harbor with a "Safe Harbor 2.0" had been underway for more than two years, but the ruling in *Schrems* caused instant havoc for businesses that relied on the mechanism as the exclusive means to legally transfer data of European citizens and set off an urgent scramble to quickly enact a replacement.

The New EU-U.S. Privacy Shield

RELATED PEOPLE

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

Tabitha K. Meier
Partner
Indianapolis

P 317-231-7326
F 317-231-7433
tabitha.meier@btlaw.com

RELATED PRACTICE AREAS

Compliance and Monitorships
Data Security and Privacy

Though the general principles of the new EU-U.S. Privacy Shield track the former Safe Harbor and general best practices for data privacy and security, the Privacy Shield will require adherence to a detailed set of standards that may surpass what U.S. law typically requires of its businesses.

The Privacy Shield specifically lays out more than a dozen privacy principles with which companies will have to comply in order to rely on the Privacy Shield as a means to legally transfer data from the EU. The seven primary principles detailed in the text are:

- Notice
- Choice
- Accountability for onward transfer
- Security
- Data integrity and purpose limitation
- Access
- Recourse, enforcement and liability

Five supplemental principles cover topics such as the handling of sensitive data, journalistic exceptions, secondary liability, the performance of audits, and human resources data.

Like the Safe Harbor before it, the Privacy Shield will require businesses to self-certify compliance with the Privacy Shield and its stated principles, which certifications must be renewed annually. Privacy Shield companies will also be required to publicly display a privacy policy consistent with the principles, one of many moves seen as furthering the Privacy Shield's emphasis on elevating the transparency of businesses privacy practices and the ways those are communicated to the public.

The Privacy Shield will also subject businesses to enhanced enforcement mechanisms and require compliance with new procedures allowing citizens to seek redress for claims of violations of the pact. The announcement revealed that the Privacy Shield will require businesses to respond to citizen complaints about their adherence to these principles within a period of 45 days. Additionally, the Federal Trade Commission and Department of Commerce's powers of enforcement will be meaningfully increased under the Privacy Shield, including providing greater authority to more closely monitor companies' privacy policies and to send detailed questionnaires as part of ongoing compliance monitoring. The Privacy Shield will also offer an arbitration mechanism to be available as a last resort option when a dispute cannot be resolved through any other means. In the EU, European Data Protection Authorities (DPAs) will be permitted to field complaints lodged by its citizens and mandates that any company that handles human resources data from Europe must commit to comply with decisions issued by the DPAs.

Related Move: Judicial Redress Act

The path to the Privacy Shield has required a number of concessions from the U.S. government. Last month, President Obama signed into law

the Judicial Redress Act, which gives citizens of foreign countries the same rights as U.S. citizens in connection with the use by the U.S. government of their personal data. Passage of this Act was seen as a critical prerequisite to passage of the Privacy Shield as it helps assuage the EU's concerns about the U.S. government's uses of personal data, a topic that loomed large in the European Court of Justice's invalidation of the Safe Harbor in *Schrems*. The U.S. Department of Justice and the Office of the Director of National Intelligence have now also provided written representations and assurances to EU authorities that any access by public authorities for law enforcement, national security, and other public interest purposes will be strictly limited and subject to clear limitations, safeguards, and oversight mechanisms. The U.S. Department of State has also been required to create a new independent ombudsperson position specifically to handle national security complaints.

Although a tentative agreement has been reached relating to the transfer and processing of personal data outside of the EU, it's still just that: tentative. Yet to be seen is whether the proposed deal is approved by various European authorities, whether any new legal challenges will arise, how any finalized Privacy Shield requirements will be implemented in practice, and what impact these new protections might have on existing data transfer mechanisms.

As a result, the ongoing uncertainty surrounding adoption of the Privacy Shield unfortunately affords no clear, immediate solutions for companies trying to understand what impact the Privacy Shield will have on their businesses and how to plan for compliance. Post-*Schrems*, in particular, many companies moved to incorporate the EU's Model Contract Clauses into their agreements as the next-best-thing to the Safe Harbor mechanism. Even now, there are still no certain answers that such clauses will be upheld or be superseded by new contractual privacy protections. Instead, companies will be forced to continue to monitor developments in connection with the Privacy Shield and closely follow first whether it is adopted, and then how it might be maintained or operated. Though we believe the Privacy Shield represents an encouraging step in the right direction, unfortunately companies are still left in the same "Safe-Harbor gap" they've been in since October. Meanwhile, business must continue and companies need to find a defendable legal strategy and mechanism if they wish to continue to collect and transfer data from Europe.

The EU Article 29 Working Party has previously indicated it will continue to honor alternative data transfer mechanisms, such as the EU model clauses and binding corporate rules, at least until it completes its assessment of the proposed Privacy Shield. Although the Working Party recognizes the efforts of the U.S. in 2014 and 2015 to improve the protection of the data of non-U.S. persons, it has previously indicated it still has concerns relating to the current U.S. legal framework for protecting certain fundamental rights and essential guarantees relating to intelligence activities, specifically scope and remedies. With the new Privacy Shield details in hand, the Working Party is currently assessing the proposed Privacy Shield, with their review expected to be completed by the end of March 2016. Certainly, without the approval of the Working Party, the Privacy Shield will find great difficulty meeting the remaining challenges to full adoption of the pact.

As we know, the invalidated Safe Harbor framework is no longer a legal

means for compliant transfers of personal information from the EU to the U.S. The Privacy Shield offers an encouraging step towards adoption of a new “Safe Harbor 2.0” system that will afford businesses the same general self-certifying mechanism to ensure legal data transfers, but at the cost of higher compliance hurdles and greater monitoring and enforcement.

Until the Privacy Shield’s fate is determined and its operation secured, businesses who need to transfer EU data remain well-advised to focus primarily on the Model Contract Clauses as the most efficient and effective means to legally transfer such data. In any event, we forecast rough waters ahead, or at the very least, choppy waters requiring careful navigation in this evolving compliance landscape.

To obtain more information regarding this alert, please contact Brian McGinnis at 317-231-6437 or brian.mcginnis@btlaw.com or Tabitha Meier at 317-231-7326 or tabitha.meier@btlaw.com.

Visit us online at www.btlaw.com and follow us on Twitter @BTLawNews.