July 2016

Shield, Sword or Plough Ahead? Approval of New EU Privacy Shield Forces a Decision.

When the European Court of Justice first invalidated the Safe Harbor we recommended here that, for most companies, staying the course by implementing general data security best practices was probably the right thing to do until the situation in the European Union stabilized.

As of last week, that interregnum in transatlantic data transfer law has ended. The EU and US governments finally signed the Privacy Shield as a replacement for the old Safe Harbor regime. Companies must now decide whether to adopt the Shield, pick up one of the weighty swords that are the other compliance methods, or plough ahead doing nothing new, waiting to see if Schrems and his supporters challenge the new arrangement as they did the old one.

What is the Privacy Shield?

- a new arrangement between the US and EU governments adopted July 2016
- replaces the old Safe Harbor arrangement held invalid by the European Court of Justice in October 2015
- is now one of the core methods for companies to comply with the EU Privacy Directive

Does my company need it?

Do you export data to the US from an EU country listed here and/or Switzerland? If you said yes, then you have to comply with the EU Privacy Directive in some manner.

How do we get it?

Companies can apply to the US Dept. of Commerce commencing August 1, 2016.

Privacy Shield is one of four (five if you include the rarely used "ad hoc clauses" method) options for achieving compliance with the EU Privacy Directive. When compared with the other methods, Privacy Shield will, using the history of its Safe Harbor predecessor as a guide, likely prove to be the most cost-effective. Using the Binding Corporate Rules (BCRs) compliance option, for instance, requires a months-long (even years-long) process. In comparison, Privacy Shield should take most companies no more than six to twelve weeks from deciding to adopt, to reaching the point of filing. Similarly, in contrast to the so-called model clauses approach, Privacy Shield is also easier to implement correctly, e.g., many companies claim to use model clauses, but few actually go deep enough in their supply chain and fewer still actually meet the Data Protection Authorities' (DPAs) local filing requirements.

So, generally speaking, we believe that unless a company has already committed to BCRs (including the requisite hefty budget accrual), the Privacy Shield is now the best option. Any credible legal challenge to the Privacy Shield may be months or even years in the making. More importantly, even if such a challenge comes and succeeds, one of the lessons learned from the Safe Harbor invalidation was that those companies that had been Safe Harbor certified were in a better position than those that had not. In the chaos that followed the Safe Harbor invalidation — when it was unclear whether any compliance method would survive — guidance from the DPAs was typically tailored to those that had been Safe Harbor certified, thus affording them some degree of certainty, but leaving everyone else with guesswork.

Those still on the fence about whether to proceed with Privacy Shield may want to consider the fact that early adopters will be rewarded with a brief reprieve from what likely will be the most burdensome element of the new Privacy Shield regime. Specifically, companies that have the Privacy Shield in place by September 30, 2016, receive the benefit of a limited grace period for compliance with the third-party-vendor contracting obligations.

What's required?

Minimally, companies will need to:

- review (or create) internal policies for collecting, securing and using personal information
- review and revise online privacy policies to meet specific Privacy Shield requirements
- put compliant contracts/addenda in place with third-party vendors
- put intracompany procedures in place with affiliates
- designate an internal contact to receive privacy-related complaints
- choose an approved dispute resolution mechanism
- confirm compliance annually through self- or third-party assessments

Rich Green
860.275.6757
rgreen@mccarter.com

Steven H. Weisman
973.848.5332
sweisman@mccarter.com

For more information on our Cybersecurity & Data Privacy practice, click here.