

Privacy and Data Security Alert: Privacy Shield Now Open for Business

August 17, 2016

For the past 15 years, over 4,000 U.S. businesses relied upon the EU-U.S. Safe Harbor program to transfer personal data from the EU to the U.S. This all came to an abrupt and surprising end on October 6, 2015, when the European Court of Justice invalidated the program and left businesses scrambling for other options to comply with EU data privacy law.

Finally, after extensive negotiations, U.S. and EU officials announced adoption of the EU-U.S. Privacy Shield as a replacement for the Safe Harbor framework. This new mechanism for cross-border transfer of data will likely become a popular choice and option for U.S. businesses. **Effective August 1, the U.S. Department of Commerce (DOC) began accepting applications from businesses seeking to self-certify under the Privacy Shield program.**

To appease EU concerns regarding government surveillance (thank you, Edward Snowden and Max Schrems), the new Privacy Shield includes a federal ombudsman to oversee intelligence access to EU citizen data, a multi-step complaint process for EU citizens, and additional enforcement and remedies for non-compliance. Similar to the Safe Harbor program, a business will be required to self-certify with the DOC as to compliance with certain privacy policies and procedures.

So what steps should a business take now if interested in Privacy Shield protection?

- Conduct a global privacy and data protection audit to better understand what data you collect, how it is used, and what steps are necessary to comply with the new Privacy Shield and any other global privacy laws such as the General Data Protection Regulation (set to become effective May 25, 2018)
- If your business was previously Safe Harbor-certified, conduct a gap analysis to determine what new steps are necessary to comply with the Privacy Shield
- Review and understand how the Privacy Shield framework operates



- Confirm your eligibility to participate

- Review and understand the privacy principles and processes required for compliance

- Develop a Privacy Shield-compliant privacy notice

- Identify an independent dispute resolution provider prior to self-certifying

- Ensure that your business has an effective process to verify and maintain compliance

- Designate an individual as contact for Privacy Shield matters

You should definitely consider adding the Privacy Shield to your global privacy compliance toolkit. Gray Plant Mooty's attorneys can help you perform a privacy audit and better understand the Privacy Shield program and the steps necessary to self-certify and comply with the program. Alternative data transfer mechanisms such as the European Commission Standard Contractual Clauses or Binding Corporate Rules should also be considered.

Additional materials, details, and guidance on Privacy Shield compliance are also available at the US Department of Commerce web site.