



EU-U.S. Privacy Shield: “Open for Business”

Aug 8, 2016

Reading Time : **3 min**

By: Natasha G. Kohne, Jo-Ellyn Sakowitz Klein, David S. Turetsky, Visiting Professor, College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University of Albany

Secretary of Commerce Penny Pritzker and EU Justice Minister Vera Jourova announced the start of Privacy Shield in a joint op-ed that highlighted the benefits that this new agreement will bring for EU citizens and U.S. businesses. The Privacy Shield includes seven principles to which organizations seeking to self-certify must commit, including a robust enforcement mechanism. The seven principles, which are detailed in the [Adequacy Decision](#) (and summarized [here](#)), are: notice; data integrity and purpose limitations; choice; security; individual access; accountability (for onward transfer); and recourse, enforcement and liability. According to the Department of Commerce, the response by businesses to the new Privacy Shield has been strong, based on the large number of applications received at the opening of the window and the range and different sizes of businesses that are applying. Below are a few implementation points to keep in mind.

Navigating the Application Process

It is important that businesses ensure that they are in compliance with the multitude of new requirements of the Privacy Shield before submitting their application. With one potential exception discussed below, “the Principles apply immediately upon certification.” For example, businesses will need to update privacy policies to reflect requirements in the notice principle that organizations provide information to individuals on the processing of personal data and the right to access that data. Also, businesses will want to ensure that they offer individuals an opportunity to opt out of the collection of their personal data where there may be disclosure to third parties or where use of the information will be materially different, but compatible with the purpose for which it was originally collected. And businesses will

need to have in place procedures to respond to individual complaints within 45 days and will need to have designated an independent recourse mechanism to investigate unresolved individual complaints, consistent with the recourse, enforcement and liability principle. Some of the changes will already be addressed in many companies existing privacy policies, but a thorough review will be critical.

Incentives for Companies Engaging in Onward Transfer

To incentivize businesses to apply early that anticipate transferring personal data to third-party controllers or processors, the Privacy Shield allows those who submit their application for self-certification within the first two months of the August 1 start date to take an additional nine months from the date of submission to ensure that their contracts for onward transfer with third parties are in compliance. Businesses that submit their application after this initial two-month window closes and that intend to engage in the onward transfer of personal data will need to ensure that all such necessary contracts are in compliance at the time of submission of the application.

New Fee Structure

In conjunction with the initiation of the application process, the Department of Commerce published the new fee structure in the Federal Register. Unlike the flat fee structure under the U.S.-EU Safe Harbor Framework, the new fee structure is tiered based on the applicant's annual revenues. The annual fees range from \$250 for businesses with revenues under \$5 million to \$3,250 for businesses with revenues more than \$5 billion. The fees have increased as compared to Safe Harbor to reflect the increased oversight and administrative role to be played by the Department of Commerce under Privacy Shield as compared to Safe Harbor.

Conclusion

The certainty that Privacy Shield brings to U.S. businesses and the assurances that it provides to EU citizens should help provide opportunities for continued growth in our shared digital economy. Please reach out to us if you have any questions regarding the EU-U.S. Privacy Shield requirements and process. One important takeaway is that there is a potentially important benefit to self-certifying and applying within the first 60 days.

Categories

Cybersecurity, Privacy & Data Protection

© 2025 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.