

Privacy & Data Security Law

:E <I #(+ D8 r#) & (-

The New “Privacy Shield”: What Does it Mean for Your Company?

This week brought important news for any company that transfers across borders, or receives cross-border transfers of, consumer or employee personally identifying data (very broadly defined). On July 12th, the [European Commission adopted the so-called "Privacy Shield" mechanism for data transfer between the European Economic Area and the US](#). US companies that choose to do so will be able to self-certify for the Shield beginning August 1, 2016. But while approval of the Shield is welcome news to many companies that relied on the [previously invalidated](#) Safe Harbor Framework, not everyone will want to take advantage of it. Alternative data transfer mechanisms still exist. And for some companies the Privacy Shield may ultimately lead to more, not less, risk. Here's a summary of what you need to consider.

What Happened - the New Shield

The Privacy Shield has been controversial, and the Commission approved it despite criticism from the [European Parliament](#), the [Article 29 Working Party](#), the [European Data Protection Supervisor](#), and numerous European data protection authorities, as well as [privacy advocates](#). In response to objections, EU and US regulators made some changes to the original draft including requirements that:

- companies delete personal data that no longer serves the purpose for which it was collected;
- certified companies include provisions in onward transfer contracts imposing obligations on the receiving company to provide the same level of protection as the certified company under the Shield Principles; and
- the appointed US Ombudsperson be independent from US national security services.

Nonetheless, [objections](#) remain, particularly regarding the ability of US authorities to obtain access to data for national security purposes. Thus, while the Shield will provide an official "replacement" Safe Harbor, its long-term value as a reliable compliance vehicle remains in question. Most significantly, European regulators can investigate data transfers irrespective

of any adequacy decision by the Commission.

Using the Shield - Pros and Cons

To certify for the Shield, you will need to self-certify annually through the Department of Commerce website in a process that is likely to be quite similar to the process companies followed for Safe Harbor.

While self-certifying is likely to be simple, participation in the Shield will subject companies to more stringent data processing restrictions, including the following:

- new complaint and redress mechanisms (and a greater likelihood of enforcement action by regulators and/or individuals via these mechanisms - on both sides of the Atlantic);
- a requirement to post a privacy policy with very specific content;
- a requirement to allow European data subjects to opt out of certain kinds of data sharing with third parties;
- a requirement to limit processing of data to only that which is "relevant" to the purpose for which it was collected, and comply with access requests; and
- a requirement to delete personal data which is no longer being used for the purposes for which it was originally collected.

Alternatives to the Shield

The Shield is not the only option for lawful data transfers. There are still other alternatives for lawful data transfer: Standard Contractual Clauses or "model clauses" (both Controller-to-Processor and Controller-to-Controller) and Binding Corporate Rules or BCRs (which do not work in a Controller-to-Processor context). Both of these alternative mechanisms are also currently subject to legal challenge, but they remain valid. While selection of a particular data transfer mechanism will depend on individual circumstances, here are some things to consider:

- Companies that have been using model clauses, particularly those that must utilize Controller-to-Processor clauses, may feel that they have already invested significant resources in putting those arrangements into place and that they would rather maintain those case-by-case contractual arrangements than adopt across-the-board data processing practices required by the Shield that are not optimal for their US business practices. Again, continuing to use model clauses is perfectly acceptable, and using those clauses will provide just as legitimate a data transfer mechanism as self-certifying for the new Shield.
- Other companies may find that they are already employing data collection, use, sharing and deletion practices that satisfy the Privacy Shield criteria. As a result, these companies may be prepared to subject themselves to the increased regulatory scrutiny that will come from self-certifying for the Shield. For these companies, the Shield may be an ideal replacement for Safe Harbor, and they will want to begin the process of updating their internal assessments of data flows to prepare for self-certification.
- Large multinationals with significant intra-company transfers may want to invest the additional time and money in obtaining BCRs, with the understanding that they will still need model clauses or Privacy Shield for Controller-to-Processor transfers.

- Some organizations may ultimately decide to relocate their data processing operations to the EU, resulting in further movement towards data localization.

We will know more once the Article 29 Working Party and individual regulators issue position statements on the Shield, and as enforcement increases. Meantime, US organizations may take comfort in knowing that all companies engaged in cross-border data transfers (for employees or customers) are subject to the same uncertainties.

If you have questions about the new Privacy Shield, or about other cross-border data transfer issues, please contact [Tanya Forsheit](#) at (310) 579 9615 or tforsheit@fkks.com, [S. Gregory Boyd](#) at (212) 826 5581 or gboyd@fkks.com, [Jeremy Goldman](#) at (310) 579 9611 or jgoldman@fkks.com, or any other member of the Frankfurt Kurnit Privacy & Data Security Group.

? D 8 5 B

New Federal Law Clarifies Foreign Governments' Immunity in Connection with Art Loans to US Museums

President Obama signed the [Foreign Cultural Exchange Jurisdictional Immunity Clarification Act](#) into law on December 16, 2016. This new law clarifies when foreign states and fine art carriers can avoid a lawsuit in the US arising from loans of culturally significant artwork to US museums. The new law is important to museums and fine art carriers, and is expected to encourage art loans by foreign states. Here's what you need to know. [Read more.](#)

JANUARY 10 2017

Ten Resolutions for a Happy and Healthy Trademark Portfolio

Here are our top ten resolutions to ensure your trademark portfolio is happy and healthy. [Read more.](#)

JANUARY 4 2017

FTC Hits Targeting Platform Turn Inc. for Deceptive Online Tracking

On Tuesday, December 20, the FTC announced a settlement with digital marketing platform Turn Inc. over claims that the company deceptively tracked users across the Internet for advertising purposes. [Read more.](#)

DECEMBER 22 2016

6 B 1 > ; ; 6 E B D # ; E B > 9 D # ; < 5 9 > # e # C 5 < J 1 # 3

New York

488 Madison Avenue
10th Floor
New York, NY 10022
P (212) 980 0120
F (212) 593 9175

Los Angeles

2029 Century Park East
Suite 1060
Los Angeles, CA 90067
P (310) 579 9600
F (310) 579 9650