

EU-U.S DATA TRANSFERS - STATE OF PLAY ON "PRIVACY SHIELD 2.0"

09/05/2022

Since the *Schrems II* 2020 judgment famously “cancelled” the EU/U.S. Privacy Shield program for personal data flows from the EU to the United States, it would be an understatement to say that U.S.-bound personal data flows from the EU have become a more complicated compliance proposition. Since data flows enable the \$7.1 trillion U.S.-EU economic relationship, this situation has received some attention at the highest levels. See [here](#) for more details on the history and findings in *Schrems II*.

It was therefore with some relief that, on 25 March 2022, the European Commission and U.S. announced that they had agreed in principle a replacement for the EU-U.S Privacy Shield; they called it the Trans-Atlantic Data Privacy Framework though it is widely (if unofficially) referred to as Privacy Shield 2.0. The Trans-Atlantic Data Privacy Framework reflects more than a year of detailed negotiations between the U.S. and EU led by US Secretary of Commerce Gina Raimondo and European Commissioner for Justice Didier Reynders.

The Current State of Play

So, what has happened since the announcement on 25 March 2022? We summarise the current progress below.

- To date there is only a statement of commitments and limited details have been provided on the new transfer mechanism itself (or the safeguards the EU will want to see for the protection of EU data subject data).
- What we have been [told](#) is that the framework marks an unprecedented commitment by the U.S. to implement reforms that will strengthen the privacy and civil liberties protections applicable to U.S. signals intelligence activities.
- To meet the concerns raised in the long-running *Schrems* litigation, the U.S. is committing to limit the signals intelligence collection it undertakes (to situations where it is necessary to advance legitimate, defined national security objectives, and does not disproportionately impact the protection of individual privacy and civil liberties).

- It will also establish a two-tier independent redress system with binding authority to direct remedial measures, to enable EU citizens to challenge access by U.S. intelligence authorities to EU personal data, in a specialist Data Protection Review Court.
- U.S intelligence agencies will also be obliged to adopt procedures to oversee new privacy and civil liberty standards for signals intelligence activities to ensure compliance with limitations on surveillance activities. .
- As before, participating U.S. companies receiving data from the EU will need to confirm their adherence to the principles set out in the new framework administered by the United States Department of Commerce (as previously, it is possible that this solution may not be available for all sectors).
- The agreement in principle is being translated into legal documents. The U.S. commitments will be included in an Executive Order that will form the basis of a draft adequacy decision by the European Commission to put in place the new Trans-Atlantic Data Privacy Framework.
- The EDPB [statement](#) on the proposals new EU-US Privacy Framework was somewhat muted, noting that there was not yet a legal framework to be assessed and highlighting that the EDPB will need to analyse the proposed reforms ‘in detail’ to check that EU citizens are afforded appropriate and effective means of redress for infringement of their privacy rights.

What does it mean for your business?

Timings for a finalised EU-U.S. framework remain unclear. The official press releases underscore the need for a “durable” solution for EU- U.S. data transfers; however, privacy advocacy groups (including that led by Max Schrems) will also be scrutinising the details once available and an early challenge to Privacy Shield 2.0 in the European courts appears likely. The legal documents are no doubt being prepared with precisely such prospective challenges in mind.

Privacy Shield 2.0 clearly has strong political support but there is still some way to go before this commitment evolves into the hoped-for durable solution for EU-U.S. data personal transfers. In the meantime, companies should continue to rely on SCCs (model clauses for data transfers – see [here](#)), not forgetting to check the status of the contractual repapering exercise required to implement the EU’s new SCCs to be completed by 27 December 2022; other transfer options may also be available under the GDPR.

The UK will also be keenly watching the progress of the Trans-Atlantic Data Privacy Framework. The UK government swiftly identified the United States as a top priority “data partnership” country post-Brexit and can be expected to look for ways to leverage (some might say “piggy back”) an EU adequacy decision for a revamped Privacy Shield program, even though EU’s recognition of Privacy Shield 2.0 would have no legal effect in the UK.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM



Anna Blest

London

anna.blest@bclplaw.com

[+44 \(0\) 20 3400 4475](tel:+442034004475)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.