ReedSmith

Client Alert

Information Technology, Privacy & Data Security

EU-U.S. Data Privacy Shield adopted – a phoenix rising from the ashes of Safe Harbor?

The EU-U.S. Privacy Shield has been adopted by the European Commission. On 12 July 2016, following a positive vote from the member states (the Article 31 Committee) on 8 July, the EU College of Commissioners formally adopted the Privacy Shield. The Privacy Shield enters into force immediately in the EU. In the U.S. the Privacy Shield will be published in the Federal Register, becoming effective on 1 August.

The Privacy Shield will be operated by the U.S. Department of Commerce, as was the now invalidated Safe Harbor Framework. In the meantime, the European Commission plans to publish a guide for European citizens explaining the remedies available to them and how such remedies may be sought, and the Article 29 Working Party (WP29), consisting of representatives from each of the member states data protection authorities, is expected to meet on 25 July 2016 to give its view on the Privacy Shield framework.

The Privacy Shield, which replaces the EU-U.S. Safe Harbor framework, will provide one of the lawful routes for transferring personal data from the EU to those U.S. organisations that have publicly self-certified compliance with the Shield's rules, by providing "adequate protection" for EU personal data.

Background and development of the Privacy Shield Last year we reported that the Court of Justice of the European Union (CJEU) struck down the Safe Harbor framework in a landmark decision in *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14). The European data protection authorities gave organisations a short 'moratorium' on enforcement until 31 January, warning that after that time they would be "committed to take all necessary and appropriate

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Cynthia O'Donoghue
Partner, London
+44 (0)20 3116 3494
codonoghue@reedsmith.com

Kate Brimsted
Partner, London
+44 (0)20 3116 3620
kbrimsted@reedsmith.com

Philip Thomas
Counsel, London
+44 (0)20 3116 3526
phthomas@reedsmith.com

Paul Bond
Partner, Princeton
+1 609 520 6393
pbond@reedsmith.com

Gerard M. Stegmaier
Partner, Washington, D.C.
+1 202 414 9293
gstegmaier@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

actions, which may include coordinated enforcement actions". As reported in February, enforcement actions were duly brought against a number of companies that had not substituted their reliance on Safe Harbor with an alternative legal basis for transatlantic data transfers.

No sooner than the Privacy Shield was announced on 2 February, doubts were raised about the robustness of the Safe Harbor replacement. The European Commission, however, published a draft 'adequacy decision' later that month, confirming its view that the replacement scheme offered adequate protection. The WP29 then released its opinion on 13 April, stating that the proposed Privacy Shield did not yet provide an adequate level of protection for personal data.

The flaws they identified were:

1. a lack of any obligation on Privacy Shield organisations to delete data if no longer necessary (i.e., lack of detail on data retention)
2. the U.S. administration did not exclude the possibility of continued massive and indiscriminate collection of data
3. the ombudsman role lacked sufficient powers to function effectively as an additional redress mechanism

In May, the European Parliament published its own resolution on transatlantic data flows, calling for the WP29's recommendations to be implemented and for Privacy Shield negotiations to be reopened to address the remaining deficiencies.

Earlier concerns addressed Perhaps unsurprisingly, the approved Privacy Shield claims to resolve the concerns raised by WP29 and the European Parliament, including:

- More explicit limits on data retention by companies: companies may keep personal data only as long as this serves the purpose the data was collected for.
- Tightened obligations in relation to onward transfers and handling by third parties of personal data provided by certified companies, including a requirement for the third party recipient to inform the Privacy Shield company when it is no longer able to ensure the appropriate level of data protection, meaning the Privacy Shield company will then have to take appropriate measures.
- Additional clarifications on bulk collection of data by the U.S. government and its agencies, in particular clarifying that it can only be used under specific preconditions and needs to be as focused as possible through using filters and the requirement to minimise collection of non-pertinent information.

- A strengthened ombudsperson mechanism, with clarification of its independence from the U.S. intelligence services and its cooperation with other independent oversight bodies with investigatory powers.
- Clarification that the Privacy Shield applies to personal data transferred from EEA member countries (Iceland, Liechtenstein and Norway), as well as EU member states.

For further information on the detailed requirements of the Privacy Shield, please see our earlier client alert here.

Should your organisation certify to the Privacy Shield? In March, we suggested that organisations with well-established consumer-facing complaints handling and engagement teams may manage the transition to Privacy Shield more easily than others.

For companies contemplating joining the Privacy Shield, it is worth bearing in mind the potential for mass (possibly coordinated) complaints by individuals to impose a heavy administrative burden on a Privacy Shield member. Companies which adopt the Privacy Shield will need to ensure they have the systems and suitable administrative bandwidth to take it on. The finalised Privacy Shield programme includes slightly greater administrative burdens for certifying companies (specifically with regard to data retention and onward transfers) than the draft released in February, and so our earlier points are even more valid.

U.S. companies that provide data processing handling services for clients, including EU-originating data, may be attracted by the recognisable 'compliance badge' aspects of the Privacy Shield programme; this will establish a Privacy Shield member as a 'safe' importer of EU data without the need for bilateral arrangements, such as EU model contract clause transfer agreements.

It is a testament to the political and economic importance of EU-U.S. data transfers that the European Commission and the U.S. Department of Commerce listened to the criticisms of the proposed Privacy Shield unveiled in February and acted rapidly to make adjustments to the framework.

Vera Jourová, Commissioner for Justice, Consumers and Gender Equality, announced that "the EU-U.S. Privacy Shield is a robust new system to protect the personal data of Europeans and ensure legal certainty for businesses" and that it "will restore the trust of consumers when their data is transferred across the Atlantic".

With the EU model contract clauses currently facing a legal challenge – also instigated by Mr Schrems – as a valid basis for transfers, as well as other EU-related changes (no legal update is complete without a reference to Brexit!), some certainty for businesses and citizens alike would be warmly received.

It is to be hoped that the extra protections introduced into the final programme will reassure privacy advocates, EU institutions and other stakeholders and allow the Privacy Shield to rise, phoenix-like, from the ashes of Safe Harbor, and remain resilient to possible future legal challenges. It has, after all, just emerged from a thorough trial. We continue to monitor the situation and will be issuing further updates as developments arise.