

April 15, 2016

Privacy Shield Takes a Hit, While GDPR Gets A Boost

The past week has seen a number of key developments in the EU data protection regime – but it has not all been smooth sailing.

First, the good news – on 8 April, the European Council formally adopted its position on the General Data Protection Regulation (“GDPR”), which will replace Europe’s current data protection regime under the EU Data Protection Directive (95/46/EC). Less than a week later, on 14 April, the European Parliament formally adopted the agreed text of the GDPR, approving the Council’s position.

The adopted GDPR text will now be published in the Official Journal of the EU and will enter into force 20 days after its publication with direct effect. Unlike the EU Data Protection Directive, individual Member States will not be required to implement national legislation to give effect to its provisions.

Back in [December 2015, we reported](#) on the key changes to be introduced under the GDPR. These include:

- a significant increase in the level of fines (maximum fines under the GDPR will be capped at the greater of EUR 20m or 4% of global annual turnover);
- wider extraterritorial jurisdiction (businesses outside Europe but offering goods and services to European citizens will be subject to the new regime); and
- increased administrative, technical and informational requirements.

Businesses that are subject to the GDPR’s much broader jurisdiction will have two years to bring their data processing in line with the requirements of the GDPR. Enforcement under the GDPR should begin in mid-2018.

Second, the bad news – for those U.S. organisations who have been closely following the developments on the EU-U.S. Privacy Shield (the proposed replacement to the Safe Harbor framework, following its [invalidation in October 2015](#)), an opinion adopted by the Article 29 Working Party on 13 April may be cause for concern and creates further uncertainty about its future.

We reported on the [proposed text of the Privacy Shield back in March](#). The hope was that the Article 29 Working Party (“WP29”) (an advisory group comprising EU national data protection authorities) would approve the Privacy Shield text, paving the way for the European Commission to formally adopt an adequacy decision on its provisions and protections. This would then provide U.S. businesses (in particular, those who previously relied on Safe Harbor to legitimise transfers of personal data to the U.S.) with an alternative to using individual consent, Binding Corporate Rules or Standard Contractual Clauses to ensure compliance with the EU data protection regime.

Despite praising the Privacy Shield as a “major improvement” over the Safe Harbor, the WP29 felt the framework fell short in the following ways:

- Commercial processing deficiencies:
 - the purpose limitation principle “is unclear and seems to open the way for reuse of data for very large purposes and transfers”;

Attorneys

[Rohan Massey](#)
[Heather Egan Sussman](#)
[Robert Lister](#)
[David T. Cohen](#)
[Matthew Coleman](#)
[James S. DeGraw](#)
[Seth C. Harrington](#)
[Douglas H. Meal](#)
[Paul D. Rubin](#)
[Michelle Visser](#)

- data retention is not referenced within the Privacy Shield and therefore does not reflect the EU principle that personal data should not be kept for any longer than is needed for the purposes for which it is collected;
- there is no mention on protections in respect of automated decision-making;
- the onward transfer mechanisms requirements are “not satisfactory” and should not allow the circumvention of EU data protection principles;
- there are too many avenues for individual recourse, and are likely to be difficult for individuals to understand and use in practice, which may lessen their effectiveness – instead, the WP29 proposes that EU individuals’ natural contact point should be their national data protection authorities; and
- there is no reference to the forthcoming GDPR (although the WP29 accepts that a review could be undertaken once the GDPR enters into force to ensure the Privacy Shield reflects the higher levels of protection it is intended to provide).
- Surveillance deficiencies:
 - mass, indiscriminate surveillance is not fully excluded, which encroaches on individuals’ fundamental rights and “can never be considered as proportionate and strictly necessary in a democratic society”; and
 - the independence and level of power the proposed ombudsperson will have within the U.S. government is still unclear.

The WP29 has urged the European Commission to address these issues in order to ensure that protections offered by the Privacy Shield are effectively equivalent to those afforded to individuals under the European data protection regime. While the WP29’s opinion is non-binding, if the Commission disregards it, this may result in a heightened chance of legal challenge against the Privacy Shield, which could result in it suffering the same fate as the Safe Harbor.

And so the uncertainty continues for a while longer. But what is clear is that businesses should not continue to rely on Safe Harbor exclusively for international transfers. The June deadline for Privacy Shield may be difficult to keep, and, if kept, the Privacy Shield may be subject to the same challenges as Safe Harbor.