Briefing

BURGES SALMON

Data protection

February 2016

Safe Harbour 2.0: The EU/US Privacy Shield

The collapse of Safe Harbour

In October 2015, we **reported** on the declaration of invalidity of the EU/US Safe Harbour regime, following the judgement of the Court of Justice for the European Union (CJEU) in the case of *Schrems v Data Protection Commissioner.*

Bridging the gap: The privacy shield

In declaring Safe Harbour invalid, the CJEU effectively removed one of the grounds for ensuring compliance with European data protection law when transferring personal data from Europe to the USA. Safe Harbour was relied upon by more than 4000 organisations as a means to self-certify compliance with European data protection law.

Following *Schrems*, the US government and European Commission held political negotiations to seek to establish a new EU-wide blanket authorisation for transfers of personal data across the Atlantic, widely regarded as being 'Safe Harbour 2.0'. The threat of intervention by national data protection authorities, in light of the regulatory hiatus since *Schrems*, added urgency to these talks and on 2 February, the European Commission **announced** the agreement of a new framework for the flow of personal data across the Atlantic, which has been branded the 'EU/US Privacy Shield'.

In making the announcement, Vice-President Ansip asserted that EU citizens can *'be sure that their personal data is fully protected', while EU businesses will have 'the legal certainty they need to develop their activities across the Atlantic'*.

Although the detailed framework is yet to be drafted, the European Commission has reported that its main provisions include:

Robust obligations on US companies processing personal data

US companies wishing to import personal data from Europe will have to publicly commit to robust obligations concerning the processing of that data and the protection of European data subjects' rights. The US Department of Commerce will ensure that these obligations are published by US data importers, meaning that they will become legally enforceable by the US Federal Trade Commission (FTC).

Restrictions on the right of US public authorities to access personal data

The US government has assured the EU that the right of US public authorities to access imported personal data for law enforcement and national security reasons will be subject to 'clear limitations, safeguards and oversight mechanisms'. In particular, a test of necessity and proportionality will be introduced, ending the indiscriminate mass surveillance of personal data in all but exceptional cases (for example where targeted surveillance is not technically possible).

To ensure US compliance with these restrictions, and to assess the functionality of the Privacy Shield generally, there will be an annual joint review between the European Commission and the US Department of Commerce.

Enforcement and redress mechanisms

EU citizens concerned about the misuse of their data will be able to complain to US companies directly or via their national data protection authority. Where complaints relate to access by US national intelligence agencies, citizens will have recourse to a new US ombudsman.

Reaction to the deal

Following the European Commission's announcement, a **press release** was issued by the Article 29 Working Party (WP29), a pan-European independent advisory body comprised of representatives from the various data protection authorities of the EU member states. The WP29 emphasised that it will need to review the documents that give effect to the Privacy Shield before commenting on its adequacy. In particular, the framework will be scrutinised against four essential requirements under European privacy law, namely:

- Processing should be based on clear, precise and accessible rules;
- Necessity and proportionality must be demonstrated, ensuring a balance between agencies' access of data and individuals' rights;
- An independent and effective oversight mechanism should exist to ensure compliance; and

- Individuals must have access to redress, to be able to enforce their rights.

Although the provisions of the EU/US Privacy Shield described by the European Commission appear to adhere to these high-level principles, questions have already arise regarding the adequacy of the Privacy Shield framework. For example: is the concept of proportionality flawed, given the disparate cultural significance attributed to privacy in America compared to Europe, and will the FTC have the authority to hold US companies to account?

The European Parliament has adopted a similar tone of caution, expressing concern about *'the value of the proposals in reality'*, including the function of the ombudsman and guarantees on judicial redress. In a **press release** dated 2 February, the European Parliament highlighted the importance of transparency, and promised to adopt the role of watchdog for citizens when discussing the new framework, implying that the Privacy Shield is far from a done deal.

What now?

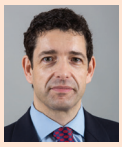
Whilst the technology community and other affected organisations will undoubtedly welcome the European Commission's announcement, many commentators are reserving judgement about the new framework until it is approved by the relevant European bodies and transcribed into a detailed and binding legal document. The European Commission will work over the next few weeks to finalise details of the arrangements, and will prepare a draft adequacy decision for formal implementation of the Privacy Shield framework but, as with the Safe Harbour framework, the Privacy Shield may still be subject to scrutiny before the CJEU.

The WP29 has called for the European Commission to communicate all documentation associated with the Privacy Shield by the end of February, so that WP29 can establish whether the Privacy Shield addresses the concerns raised by the CJEU in the *Schrems* judgment. The WP29 intends to hold an extraordinary meeting by early April to decide upon the means by which personal data can be transferred to the US in compliance with European privacy law.

Consumer confidence in the transatlantic flow of data also remains an area of commercial concern for businesses, which may affect the extent to which personal data is transferred from European to American entities by virtue of the Privacy Shield arrangement.

Pending the legalisation of the EU/US Privacy Shield, organisations transferring personal data to the USA should incorporate model data protection clauses into the contracts governing those transfers or, in respect of intra-group transfers of data, seek to establish corporate rules that safeguard data subjects' rights. Whilst this remains the approach recommended by the WP29, organisations should remain alert to any change in guidance that may follow.

Contact



Andrew Dunlop
Partner

+44 (0)117 902 2786
andrew.dunlop@burges-salmon.com

David Varney
Associate

+44 (0)117 902 7261
david.varney@burges-salmon.com