

Privacy Shield under fire

Pulina Whitaker, partner, Morgan Lewis
16th May 2016

The proposed EU-US Privacy Shield, intended to facilitate transatlantic data transfers, has been thrown into doubt by the Article 29 Working Party's Opinion, released on 13th April 2016, which concluded that it does not meet EU data protection standards. The Article 29



Pulina Whitaker
Partner, Morgan Lewis

Working Party, which advises the European Commission on data protection matters, does not release binding opinions, but they are heavily influential. The European Commission can choose to ignore this Opinion or, more likely, address the concerns and revise the draft proposal. Subject to this, the next formal stage is the Article 31 Committee vote which is binding.

Safe Harbour invalidated

According to the European Commission, the United States is a country with “inadequate” data protection laws. In 2000, the European Commission and the US Department of Commerce, therefore, agreed to implement a self-certification programme for US organisations to receive personal data sent from Europe provided the US organisations certified that they adhered to certain standards of data processing comparable with EU data protection laws so that EU citizens' personal data was treated as adequately as if their personal data had remained within Europe. This Safe Harbour programme was operated by the US Department of Commerce and enforced by the Federal Trade Commission.

The European Commission considered strengthening the Safe Harbour programme following Edward Snowden's revelations that the US security services were collecting and using the personal data of EU citizens on a large scale. A law student, Maximillian Schrems, complained, in Irish legal proceedings, that the Irish Data Protection Commissioner refused to investigate his complaint that the

Safe Harbour programme failed to protect adequately personal data after its transfer to the US in light of Edward Snowden's revelations.

The question of whether EU data protection authorities have the power to investigate complaints about the Safe Harbor programme was referred to the Court of Justice of the EU (ECJ). The ECJ ruled, in October 2015, that the European Commission decision approving the Safe Harbour programme was invalid. Further, the ECJ ruled that EU data protection authorities can investigate complaints about the transfer of personal data outside Europe and, where necessary, suspend such data transfers until those investigations are satisfactorily completed. The ECJ also found that EU citizens do not have adequate rights of redress where their personal data protection rights are breached by US authorities which undermines their European data protection rights.

Proposed Privacy Shield

On 29th February 2016, the European Commission published a draft adequacy decision to establish the EU-US Privacy Shield, the replacement for the invalidated Safe Harbour programme. The EU-Privacy Shield would be operated by the US Department of Commerce and enforced by the Federal Trade Commission, as was the Safe Harbour programme.

The publication of the draft adequacy decision was initially welcomed by the Article 29 Working Party. Following a review of the documentation, the Article 29 Working Party expressed significant concerns that the draft proposal does not give enough protection to European citizens because "...massive and indiscriminate data collection is not fully excluded by the US authorities and..the powers and position of the Ombudsman have not been set out in more detail." The Article 29 Working Party was concerned that a number of important data protection principles have not been expressly incorporated within the EU-US Privacy Shield, including:

- it does not have a data retention principle;
- there seemed to still be a risk of massive and indiscriminate collection of personal data for national security purposes; and
- the legal remedies were insufficient, particularly in relation to the Ombudsman remedy, whose independence and specific remit was questioned by the Article 29 Working Party.

The Article 29 Working Party also identified that there is no mechanism for updating the EU-US Privacy Shield once the General Data Protection Regulation comes into force on 25th May 2018.

The Article 29 Working Party has not, however, rejected the proposal, but has instead requested that the European Commission clarifies the drafting of the proposal and resolves the outstanding concerns

about adequately protecting personal data. Isabelle Falque-Pierrotin, chair of the Article 29 Working Party and head of France's data protection authority, CNIL, recognised during a press conference that the EU-US Privacy Shield was a "great step forward" compared to the previous Safe Harbour program.

Next steps

The European Commission is not bound by the Article 29 Working Party's opinion and could still, therefore, formally adopt the draft adequacy decision notwithstanding the Article 29 Working Party's concerns. A more likely outcome is that the European Commission will now revise its decision in order to address the Article 29 Working Party's concerns. If so, this is likely to require further negotiations with the US authorities. Accordingly, it seems unlikely that the EU-US Privacy Shield will be adopted in June 2016 as originally anticipated.

Alternative EU-US data transfers

In the meantime, there are other options to transfer personal data to the US, including express consent and the use of Binding Corporate Rules or EU-approved model clause agreements. Organisations with Safe Harbour certification or who use Safe Harbour-certified vendors should consider these options or discuss these other options with their vendors.

Model clauses are very commonly used. Other than in a few European countries such as Cyprus and Greece, there is no requirement to obtain a specific permit from the data protection authority to use model clause agreements.

There is, however, a risk that the Schrems decision could affect these other options of transferring personal data outside the European Economic Area. Other countries, as well as the US, have national security derogations which are likely to override the protection of personal data however it is transferred, with the only exception of specific and informed consent from an individual to the transfer of his or her personal data to governmental authorities for national security purposes.

In the meantime, companies should continue to rely on the Standard Contractual Clauses and Binding Corporate Rules for their EU-US data transfers. These have been expressly approved by the Article 29 Working Party as remaining valid (for now).

This article was originally published in **DataIQ**.

The online version can be [found here](#).