The EU-US Privacy Shield — is it strong enough?

Alison Deighton, Partner at TLT LLP, considers whether the European Commission's announcement of a new EU-US Privacy Shield offers a real solution for US data transfers

The decision of the Court of Justice of the European Union in the Schrems case (*Maximilian Schrems v Data Protection Commissioner,* Case C-362/14) resulted in huge upheaval and uncertainty for businesses that transfer personal data to the United States.

Much of the commentary regarding the decision has focused on the impact for technology giants and global corporations. However, the impact of the decision goes far wider, requiring any organisation that transfers personal data to the United States to examine the basis of their transfers and to put in place alternative mechanisms to ensure adequate protection where Safe Harbor had been relied upon.

The decision also called into question the validity of other transfer mechanisms, potentially affecting all organisations relying on them.

The announcement on 2nd February 2016 that the European Commission and the United States had agreed a new framework for transatlantic dataflows (the fantastically named 'Privacy Shield') therefore came as welcome news. But, does the Privacy Shield meet the requirements to ensure adequate protection for the fundamental right to privacy of EU citizens? What are the regulators saying? And what should organisations be doing in practice in relation to their data transfers to the United States?

Key findings in the *Schrems* judgment

Before examining these questions, it is worthwhile reminding ourselves of the key findings of the Court of Justice of the European Union ('CJEU') in the Schrems judgment.

The CJEU ruled that the European Commission's decision that the Safe Harbor regime offered an adequate level of protection for personal data was invalid. The decision was based on the following factors:

- **In order for an adequacy decision to be made by the European Commission, the 'legal order' of the relevant country must provide an adequate level of protection that is equivalent to the protection offered by European Union law** — In accordance with Article 25(6) of the Data Protection Directive (95/46/EC) the 'legal order' includes domestic law or 'international commitments'.
- **While a self-certification regime may be an adequate mechanism for ensuring protection, there must also be effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights** — In particular, the right to respect for private life and the right to protection of personal data, to be identified and enforced in practice.
- **The Safe Harbor principles only bind those organisations that self-certify that they comply with the principles** — US public authorities are not obliged to comply with them.
- **The European Commission made no finding regarding the existence in the US of any rules to limit interference with fundamental rights of EU citizens** — Also, the decision did not refer to the existence of effective legal protection for individuals against interference of that kind.
- **Any laws enabling interference with the fundamental rights to privacy must lay down clear and precise rules governing the scope and application of a measure, and must impose minimum safeguards** — This is so that the persons whose personal data are affected have sufficient guarantees enabling their data to be effectively protected against the risk of abuse, and any unlawful access and use of that data.
- **Protection of the fundamental right to respect for private life requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary**.
- **Having adopted an adequacy decision, the Commission must periodically check whether the decision is still factually and legally justified.**

In order for the European Commission to be able to make an adequacy decision in relation to the proposed Privacy Shield, the Commission will therefore need assurance that the Privacy Shield meets each of these requirements.

Does the Privacy Shield meet EU requirements?

On 29th February 2016, some further details on how the Privacy Shield will be put into effect in US law were released (via a European Commission adequacy decision and a set of other documents, all available via the Commission's webpage — see www.pdpjournals.com/docs/88510). The Privacy Shield will include the following elements:

- strong obligations on companies handling Europeans' personal data and robust enforcement;
- clear safeguards and transparency obligations on US government access; and
- effective protection of EU citizens' rights with several redress possibilities.

US companies wishing to import personal data from Europe will need to commit to robust obligations on how personal data are processed and individual rights are guaranteed.

The Department of Commerce will monitor companies publishing their commitments, which makes them enforceable under US law by the Federal Trade Commission. In addition, any company handling human resources data from Europe is required to commit to complying with decisions by European data protection authorities. Provided that there is a clear legal basis to enforce data protection obligations on US organisations that self certify, it seems likely that the Privacy Shield will be capable of satisfying the requirements set out in the *Schrems* judgment in relation to enforceability and punishment for organisations that fail to comply with Privacy Shield requirements.

"While regulators are — for the most part — taking a pragmatic approach to enforcement, there is nothing to stop privacy activists from making complaints to regulators or taking action before national courts. It is also clear that organisations that are continuing to rely on Safe Harbor are at risk of enforcement action."

In relation to redress mechanisms, the press release specifies that any citizen who considers that their data have been misused under the new arrangement will have several redress possibilities. Companies will have deadlines to reply to complaints. European data protection authorities will be able to refer complaints to the Department of Commerce and the Federal Trade Commission. In addition, alternative dispute resolution will be free of charge.

For complaints on possible access by national intelligence authorities, a new Ombudsperson will be created. Again, provided that the US implements measures that have legally binding effect on US organisations (including public authorities), the Privacy Shield will be able to satisfy European requirements in relation to redress for individuals.

One more problematic issue arises in relation to US government access to data relating to EU citizens. The US has given the EU 'written assurances' that public authorities' access for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. These exceptions must be used only to the extent necessary and proportionate. The US has 'ruled out indiscriminate mass surveillance on the personal data transferred to the US under the new arrangement'.

Privacy activists have already expressed concern that mere assurances will not be sufficient to protect the right to privacy. The draft adequacy decision published by the European Commission sets out in detail the various mechanisms through which the US ensures that appropriate limitations are placed on access and use of personal data by US public authorities. Much emphasis is placed on Presidential Policy Directive 28 issued by Barack Obama on 17th January 2014. This Policy Directive binds US intelligence authorities and places restrictions on the way in which surveillance activities must be conducted. Tellingly, however, the Policy Directive does not bind Congress and could be superseded by subsequent Policy Directives issued by the next administration.

It will be interesting to see whether European Data Protection Authorities can make themselves comfortable that the Policy Directive together with a 'written assurance' will amount to 'an international commitment' as required under the Directive to enable an adequacy finding.

If concerns are raised about the binding nature of these commitments or if/when there are policy changes in the future, it is highly likely that any new arrangements for transatlantic data flows will be subject to exactly the same challenge as Safe Harbor.

What are the regulators saying?

Following the release of the details of the Privacy Shield, the Article 29 Working Party will carry out its own assessment as to whether the Privacy Shield overcomes concerns relating to the US legal framework in the context of surveillance activities. The Article 29 Working Party has identified four 'essential guarantees' that need to be in place in relation to surveillance activities:

Processing should be based on clear, precise and accessible rules — This means that anyone who is reasonably informed should be able to foresee what might happen with her/his data where they are transferred.

Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated — A balance needs to be found between the objective for which the data are collected and accessed (generally national security) and the rights of the individual.

An independent oversight mechanism should exist, that is both effective and impartial — This can either be a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks.

Effective remedies need to be available to the individual — Anyone should have the right to defend her/his rights before an independent body.

The Article 29 Working Party has made it clear that these guarantees need to be in place for all overseas data transfers, regardless of the mechanism used to ensure adequate protection.

The Article 29 Working Party will also be examining whether the Privacy Shield will provide legal certainty for other transfer tools, as well as for those organisations that sign up to the new Privacy Shield arrangements.

The stakes are high; if the Privacy Shield does not stand up to scrutiny by the European data protection authorities in relation to the four 'essential guarantees', all data transfers to the US will be in jeopardy.

What will happen next?

The draft adequacy decision could be adopted in its current form following the advice of the Article 29 Working Party—or adapted in line with recommendations.

Since a committee of representatives of the Member States will also need to be consulted, it would seem that we are still some weeks away from a final deal.

What steps should organisations take now?

Although the European Commission has found the Privacy Shield to offer adequate protection, it is likely to be some time before organisations transfer to the new scheme and put in place appropriate policies and procedures to comply with more robust data protection requirements.

In the meantime, organisations transferring data to the US continue with the threat of potential legal action. Even if businesses are not relying on Safe Harbor, the underlying reasons for the invalidity of the Safe Harbor decision apply equally to other transfer mechanisms.

While regulators are — for the most part — taking a pragmatic approach to enforcement, there is nothing to stop privacy activists from making complaints to regulators or taking action before national courts. It is also clear that organisations that are continuing to rely on Safe Harbor are at risk of enforcement action.

There is no easy answer. However, organisations should ensure that they are taking the following steps to protect their position so far as possible:

- Continue to audit all data transfers to identify where data are being transferred to the US, and keep a log of all transfers;
- Until the Privacy Shield receives formal adequacy approval, ensure that alternative mechanisms to Safe Harbor for transferring data to the United States are in place, such as using the Model Contractual Clauses;
- Consider whether any exemptions to the requirement to ensure adequate protection can be relied upon. For example, is it feasible to obtain individual consent to the transfer? Is the transfer necessary in order to fulfil a contractual commitment?; and
- As part of an ongoing audit, assess the nature of the data being transferred to the US to allow the identification of high risk transfers and a consideration of the alternative options if the Privacy Shield is not approved, or is subject to future legal challenge.

Alison Deighton
TLT LLP
alison.deighton@TLTsolicitors.com