EU-US Privacy Shield to replace US Safe Harbour

9 February 2016

On 2 February 2016, the EU Commission announced that it had reached political agreement with the US Department of Commerce on a revised Safe Harbour scheme.

Key elements of the deal

Vera Jourová, EU Commissioner for Justice, Consumers and Gender Equality, introduced the revised US Safe Harbour scheme, rebranded as the 'EU-US Privacy Shield', at a press conference on 2 February. The deal has been agreed at political level only, following months of intense negotiations with the US Department of Commerce. Vera Jourová highlighted some of the key aspects of the agreement reached, including:

- **Binding written assurances from the US that the access to personal data by US public authorities 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;
- **Redress rights for European citizens**, including the referral of complaints by EU data protection authorities ('DPAs') to the Department of Commerce and the Federal Trade Commission (the 'FTC'), deadlines for companies to respond to complaints, free alternative dispute resolution for EU Citizens and a new dedicated Ombudsman to deal with complaints on possible access to personal data by intelligence authorities;
- **Regular reviewing and monitoring.** The EU Commission will conduct a joint annual review of the Privacy Shield with the Department of Commerce. The Department of Commerce will monitor that the US companies publish the required commitments (which will be enforceable under US law by the FTC); and
- **Strong obligations on companies handling Europeans' personal data**. US companies importing personal data from EU countries under the Privacy Shield will need to commit to robust obligations on how personal data are processed and individual rights are guaranteed. They will also have to comply with decisions by European DPAs.

Background

On 6 October 2015, the EU Commission's decision on the adequacy of the US Safe Harbour was declared invalid by the Court of Justice of the European Union in the Schrems case.

Recognising the uncertainty and disruption this would cause to companies on either side of the Atlantic (and more widely, to all transfers of personal data outside of the EEA), the EU data protection authorities then issued an ultimatum to EU and US politicians, requesting a resolution by 31 January 2016.

Timing

The Privacy Shield has only been agreed in principle. The EU Commission still needs to prepare a draft adequacy decision which "could then be adopted [by the Commission] after consulting a committee composed of representatives of the Member States". In the meantime, the US still has to make arrangements to put in place the new framework, monitoring mechanisms and new Ombudsman.

As yet, there is no further guidance for companies that had self-certified under the original Safe Harbour as to what they will need to do to ensure they come under the umbrella of the new EU-US Privacy Shield.

Reactions from EU DPAs

The EU regulators met on 2 and 3 February, through the medium of the Article 29 Working Party (the 'A29WP'), to discuss the consequences of the Schrems judgement and the new EU-US Privacy Shield.

Much of the detail of the new Privacy Shield framework is still missing, so it is perhaps not a surprise that the A29WP has called on the EU Commission to provide it with the necessary paperwork and documents relating to the new framework, by the end of the February, to enable it to properly asses the agreed deal. The A29WP identifies four criteria against which it will judge the Privacy Shield:

- Processing should be based on clear, precise and accessible rules - i.e. a reasonably informed person should be able to foresee what might happen with their data;
- Necessity and proportionality - i.e. there has to be a demonstrable balance between the objective for which the data are collected and accessed (generally national security) and the rights of the individual;
- Independent oversight mechanisms should be in place (such as a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks); and
- Effective remedies need to be available to the individual.

The A29WP is currently not convinced that the new Privacy Shield meets these criteria, in particular in relation to scope and remedies.

It should be noted that the US Senate Judiciary Committee passed the Judicial Redress Act on 28 January 2016. The Act still needs to go to the Senate in plenary and, crucially, certain amendments have been added which appear to impose additional conditions on the rights of EU citizens to obtain legal redress in the US. It remains to be seen how this will affect the final approval of the EU-US Privacy Shield.

The A29WP states that the deadline of 31 January has been met, which presumably means that EU DPAs will not be taking immediate co-ordinated legal action against non-compliant data controllers. Rather, individual DPAs will take action on a case by case basis where appropriate.

What should companies do until the Privacy Shield is formally adopted?

Organisations that transfer or receive personal data out of the EEA will be encouraged by the A29WP's confirmation that existing mechanisms such as Binding Corporate Rules or EU standard model clauses can continue to be used for transfers to the US (and elsewhere out of the EEA) for now. However, once the A29WP has assessed the Privacy Shield in detail, it will then consider whether, in its opinion, these alternative transfer mechanisms meet the relevant criteria.

This means that the current uncertainty surrounding international transfers has not been completely removed and is unlikely to be dealt with for at least a few months.

Conclusion

The Privacy Shield presented by the EU Commission on 2 February does not appear to be substantially different to the original Safe Harbour, although the exact extent to which it differs will become clearer as the details of the scheme are worked out and made public.

Representatives of the digital technology sector and ISPs such as DIGITALEUROPE and EuroISPA have voiced their support of the new Privacy Shield and the A29WP's view that alternative mechanisms can continue to be used for now. However, others (such as Jan Albrecht, German MEP and the EU Parliament's rapporteur for the General Data Protection Regulation) are clearly unimpressed. What is clear is that many will be waiting to closely scrutinise the precise nature and significance of some of the commitments provided by the US in relation to access to data for the purposes of national security and the rights of redress granted to EU citizens. If these do not prove to be sufficiently effective and robust, it is difficult to see how the EU-US Privacy Shield will be formally approved and allowed to function without challenge.

Rebecca Cousin
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Rob Sumroy
T +44 (0)20 7090 4032
E rob. sumroy@slaughterandmay.com

9 February 2016