**Briefing: EU – U.S. Privacy Shield**

**July 2016**

**Q. What was the Safe Harbour framework?**

A. The European Data Protection Directive ([Directive 95/46/EC](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046)) generally prohibits the transfer of personal data from the EU to countries outside the European Economic Area (EEA) unless the European Commission (EC) has decided that the data protection rules of the third country provide ‘adequate’ protection in relation to personal data.

The European Commission – in consultation with the US Department of Commerce – adopted the Safe Harbour principles ([Decision 2000/520/EC](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML)) in July 2000. The decision allowed registered companies to transfer personal data from the EU to the U.S.

**Q. So what happened to the Safe Harbour framework?**

A. On 6 October 2015, [the Court of Justice of the European Union (CJEU) invalidated Safe Harbour](http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=7666), arguing that it had enabled *‘interference (...) with the fundamental rights [to privacy and judicial redress] of the persons whose personal data is or could be transferred from [the EU to the U.S.]’*. Additionally, the CJEU found that Safe Harbour wrongfully limited the power of national data protection authorities (DPAs) – such as the Information Commissioner’s Office (ICO) in the UK – to investigate claims by individuals concerning the adequacy of third countries.

**Q. Is a successor to Safe Harbour in place yet?**

A. Yes. On 12 July 2016, the EC formally [adopted](http://europa.eu/rapid/press-release_IP-16-2461_en.htm) the EU-U.S. Privacy Shield, the successor to the Safe Harbour agreement.

**Q. What are the differences between the Privacy Shield and Safe Harbour?**

A. In essence, there aren’t many. The main updates include further obligations placed on U.S. companies that transfer EU citizens’ data (as well as ensuring enhanced oversight of their compliance), written assurances from the U.S. Government that access to personal data will be limited to specific conditions and the establishment of new redress mechanisms.

Full details of the framework, the obligations for businesses transferring data and the redress mechanisms, plus the legal texts are available on the [European Commission website](http://europa.eu/rapid/press-release_IP-16-2461_en.htm).

**Q. Does the Privacy Shield address the problems of Safe Harbour identified by the CJEU?**

According to the EC, “The EU-U.S. Privacy Shield reflects the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbour framework invalid.” The Privacy Shield includes what the EC describes as ‘stronger obligations’ for US companies transferring data, including requirements to cooperate with EU DPAs, plus provisions intended to address concerns about mass surveillance and the process for consumer complaints.

Some privacy advocates and policymakers, however, have already questioned whether the Privacy Shield goes far enough to address the concerns identified by the CJEU, making it likely that the new framework will be subject to a legal challenge in Europe, in the same fashion as the one that brought down Safe Harbour.

**Q. Can I start to transfer data to the U.S. under the Privacy Shield framework?**

A. Not yet. As with Safe Harbour, businesses will be required to self-certify and to register annually with the U.S. Department of Commerce, which will maintain an up-to-date list of Privacy Shield members. Registration opens on 1 August 2016.

**Q. Are there any alternatives to the Privacy Shield for transferring data to the U.S.?**

A. Adequacy decisions are not the only mechanism allowing the transfer of personal data from the UK to the U.S. Businesses may still use any one or several of the following alternatives (follow links for further details from the ICO):

* [(Self-) assessing adequacy for international data transfers](https://ico.org.uk/media/1529/assessing_adequacy_international_data_transfers.pdf)
* [Model Contract Clauses for international transfers of personal data](https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf)
* [Binding Corporate Rules (“BCRs”)](https://ico.org.uk/for-organisations/binding-corporate-rules/)
* Derogations of Art. 26(1) Data Protection Directive, including the consent of the data subject (under certain conditions)

Companies operating in other EU Member States should consult the relevant data protection authorities in those markets as requirements for the lawful transfer of personal data vary across countries.

**Q. How do I stay up-to-date?**

A. IAB UK will update this briefing paper to reflect any further developments. It is recommended that organisations seek their own legal advice to ensure measures are in place to allow for the legal transfer of data from the UK to the U.S.

**For further information contact Yves Schwarzbart, Acting Head of Policy & Regulatory Affairs, at yves@iabuk.net or visit the** [**policy briefings**](http://www.iabuk.net/policy/issues) **section on our** [**website.**](http://www.iabuk.net/)

*IAB UK, July 2016*