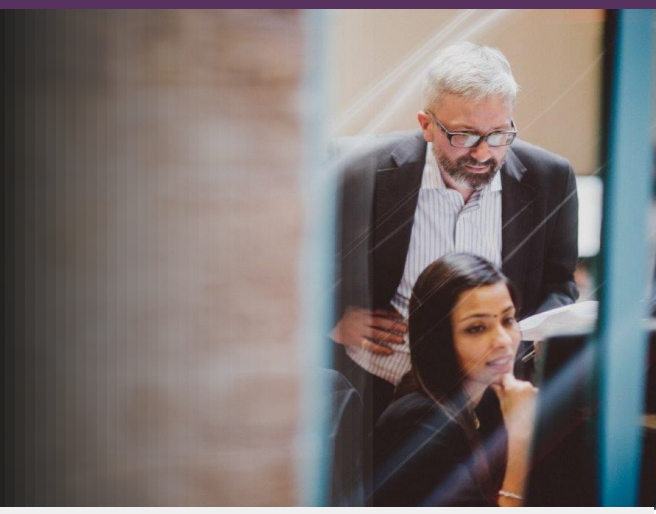
RIAA Barker Gillette

Always Available

Data transfers: EU/US Privacy Shield shattered



July 2020

On 16 July 2020, the Court of Justice of the European Union (CJEU) struck down the European Union (EU)/United States (US) Privacy Shield, which served as the mechanism for which EU citizens' personal data could be shared with US. Instead, companies must now use standard contractual clauses (SCCs).

This will have far reaching impacts on companies on both sides of the pond where those that relied on the privacy shield to transfer such personal data will now have to find an alternative method or otherwise stop. This development will prove to be extremely problematic for companies that work across both jurisdictions who must transfer personal data for their company to function.

What was the Privacy Shield?

Companies can transfer personal data to other countries where there is at least an equal measure of data protection as that directed by EU law. Companies can legally transfer data where the EU has determined a third country has adequate measures in place. The US has not passed this test owing to substandard data protection and privacy laws and so the EU and US produced the framework known as the Privacy Shield. This framework carved out a legal path by which the personal data of EU citizens could be transferred between the EU and US, so long as those US companies enrolled to the Privacy Shield and complied with the data protection obligations imposed upon them.

Why did the CJEU invalidate the Privacy Shield?

The CJEU determined that US National Security law does not sufficiently protect EU citizens' personal data given surveillance laws in the US which allow the government to access more personal data than what is strictly necessary. In short, the US government can snoop to a degree which does not sit well with EU law. Hence, personal data transferred under the Privacy Shield framework is not sufficiently protected.

Standard Contractual Clauses – what are they?

SCCs are standard clauses which are published by the European Commission or by a member state Supervisory Authority and, where used, offer sufficient safeguards on data protection to allow the personal data to be transferred outside of the EU. Although the CJEU endorsed the use of SCCs moving forward, it made clear that parties have an obligation to ensure that the laws in the recipient country are sufficient to protect EU personal data and if the guarantees of the SCCs are not upheld then personal data transfers with that company must be suspended.

What should companies do now?

Companies that transfer personal data to the US must ensure they continue to do so lawfully. Where a company has previously relied on Privacy Shield certification they must put in place a new transfer mechanism which should be in the form of an SCC but, where required consider additional, supplemental contractual safeguards which go above the standard SCCs.

To avoid falling foul of the Information Commissioners Office (ICO) companies must now act to assess whether their data privacy safeguards are sufficient and ensure those of any company outside of the EU with whom they have or intend to continue sharing EU citizens' personal data affords an equivalent protection guaranteed within the EU under GDPR legislation.

This is a complicated area of cross border data protection law and an area where companies are best erring on the

side of caution and seeking advice from a qualified lawyer to ensure their compliance with EU law.

Speak to Karen Cole today who can review your existing contracts and practices to ensure your company is compliant.

Karen Cole
07903 619 001
karen.cole@riaabg.com
www.riaabarkergillette.com

Click here to make an online appointment