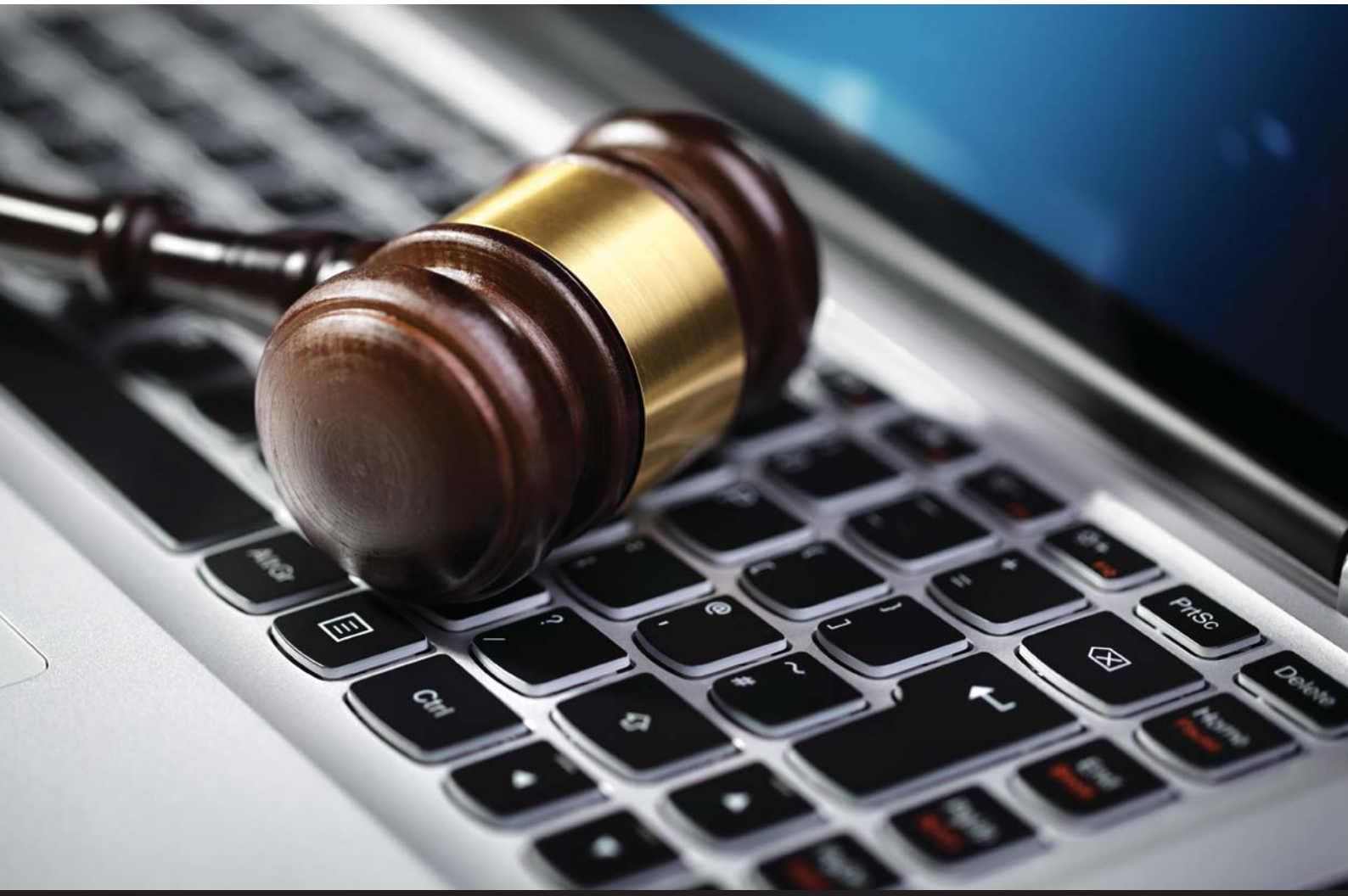
OCTOBER 2015

blackfoot

BLACKFOOT NEWSFLASH



NO SAFE HARBOUR

What now for sharing personal data with the US?

On 6th October the European Court of Justice ruled that the EU/US Safe Harbour agreement — a long-standing arrangement that facilitates sharing of personal data between EU and US organisations — is invalid and can no longer provide adequate protection for data transfers.

The ruling marks the culmination of a long-running dispute between an Austrian student, Max Schrems, and Facebook. Schrems argued successfully that the Irish Information Commissioner must investigate Facebook's transfer of personal data from Facebook's Irish servers to the US, where privacy laws are not deemed 'adequate' to protect EU citizens' data.

This is the most significant legal impact of the revelations from NSA whistleblower Edward Snowden, since his evidence of mass interception of private sector data by US authorities was cited as a violation of Schrems' privacy rights.

The European Court of Justice's decision will force the Irish Information Commissioner to investigate Facebook, but more importantly it means that the 4,000 organisations relying on Safe Harbour to provide legal means to transfer personal data to the US (either to partners or within the organisation) are technically in breach of the law and must urgently find an alternative legal means.

Other mechanisms open to them include model contracts and binding corporate rules, both of which have the effect of forcing US entities to process data under EU rules.

Implications of the decision

The implications of this decision must not be underestimated: the immediate impact is that companies such as Apple, Facebook and Google are in breach of EU law, but we've not seen their services switched off. Data protection authorities must now come up with a strategy for how — and when — to enforce the ruling, and organisations must be ready for that deadline, which is likely to vary from country to country.

And the fight is not yet over: Schrems will likely argue that any transfer of personal data to the US, regardless of the protection mechanism used, is illegal, and he will, in all probability, succeed in doing so. That dispute might take years to play out, but in the meantime the US is already furious at the situation, and US companies will be demanding a change to their domestic laws, including controls over surveillance activities, so that they can compete effectively in Europe. Politicians, lawyers and lobbyists have a busy few years ahead.

In the meantime, organisations need to manage their own risks arising from the situation. In the first instance, they need to:

Assess what data transfers within or outside of the organisation — if any — they carry out using Safe Harbour, and implement alternative legal mechanisms

Review supplier and third party contracts (with priority for those that are pending approval or renewal) to understand whether those suppliers or third parties, or their supply chains, rely on Safe Harbour, and seek alternatives where there is a risk to the supply chain

Take a strategic long-term view on how, and where, they intend to manage personal data in future, given the uncertainty about the long-term relationship between the EU and the US

There is also a huge opportunity here for EU companies wishing to compete with the US. Buyers are unlikely to want to risk signing up for US-hosted services whilst the future is so uncertain, and nimble European competitors will be seen as a much safer option.

For more information

If you would like to discuss the decision, and how it affects your organisation, please contact your Blackfoot account manager.

blackfoot

Blackfoot UK Limited
Tel: 0845 805 2409
E-mail: info@blackfootuk.com
Web: www.blackfootuk.com

ADVISE >
ASSESS >
ASSURE >