CYBER RISKS

NO SAFE HARBOR FOR DATA STORED IN USA

Maximillian Schrems v Data Protection Commissioner

Current EU position on data transfer.

Data protection within the EU is regulated by EU Directive 95/46/EC. Article 25 provides that the transfer of personal data to a third country may take place only if that country ensures an adequate level of protection. The Commission may make a finding that the third country ensures an adequate level of protection as a result of its domestic or international commitments. Each Member State must designate a national supervisory authority (NSA) responsible for monitoring the application of the Directive within its territory.

Commission decision 200/520/EC

Article 1 of 200/520/EC provides that adequate protection is provided by US undertakings which self-certify their adherence to the Safe Harbor principles, which are broadly similar to the principles in Directive 95/46/EC. US organisations which sign up to and comply with the Safe Harbor programme are automatically authorised to accept data transfers from the EU without the need for individual approval or compliance with other legal or regulatory requirements.

The Snowden effect

The Safe Harbor principles, which are intended to ensure an adequate level of protection for data transferred to the US, contain an exception whereby if there is a conflicting statute, regulation or case law obligation, US organisations must comply with US law. This allows US public authorities, who are not required to comply with Safe Harbor, to access an individual's data without limitation.

In 2013 Edward Snowden made significant revelations about the US National Security Agency surveillance of data held by Safe Harbor participants, which severely undermined Safe Harbor's credibility as a system which protected an individual's data to a level essentially equivalent to that guaranteed within the EU under Directive 95/46/EC. Although there were negotiations between the EU and US to address the situation, decision 200/520/EC was not retracted.

Maximillian Schrems

Mr Schrems, an Austrian national, had been a facebook user since 2008. As with other subscribers residing outside the US, at the time of registration Mr Schrems entered a contract with Facebook Ireland, a

subsidiary of Facebook Inc. established in the US. That contract provided that some or all of the user's personal data would be transferred from Ireland to the US where it would be processed. Mr Schrems made a complaint to the Irish Data Protection Commissioner (DPC) asking it to use its power to prevent the transfer of his data to the US as their law and practice did not provide adequate protection of his data. The DPC took the view it could not deal with the complaint, particularly as it was bound by decision 2000/520/EC. Mr Schrems took the complaint to the High Court of Ireland.

The Charter of Fundamental Rights of the EU (the Charter) protects EU citizens' rights to respect for private life (article 7), the right to protection of personal data (article 8) and the right to an effective remedy and fair trial (article 47). The High Court considered that although electronic surveillance of personal data transferred to the US did serve a necessary objective in the public interest, there had been a significant over-reach on the part of some US federal agencies. In addition, the Court found that EU citizens had no effective right to be heard as part of US oversight proceedings. The High Court referred the matter to the ECJ to determine whether it was bound by decision 200/520/EC, having regard to Articles 7, 8 and 47 of the Charter, or whether the DPC could conduct its own investigations into the matter.

ECJ Decision

In a decision handed down in October 2015, the Court held that decision 200/520/EC on Safe Harbor was invalid for the following reasons:

US national security, public interest and law enforcement requirements of the US override the scheme so that where there is a conflict, the US is able to disregard without limitation the protective rules laid down by the scheme. The Court held that this compromised the essence of the fundamental right to respect for private life.

The persons concerned had no administrative or judicial means of redress enabling the data relating to them to be accessed and either rectified or erased. This compromised the essence of the fundamental right to effective judicial protection.

The Safe Harbor decision denied the NSA their powers when a person called into question whether the decision was compatible with the protection of privacy and freedoms of the individual. The Commission did not have the competence to restrict the NSA, who must be able to examine a transfer to a third country with complete independence.

CPB Comment

This decision will have an enormous impact on the more than 4,500 companies signed up to the self-certification Safe Harbor regime. Although international data flow is extremely important, transfers taking

place under the regime are now considered unlawful and companies need to find alternative legal grounds for data exports from the EU to the US until a solution can be reached.

Although a new Safe Harbor package is being negotiated there is no timeframe for finalising this and it could be some time before there is a workable arrangement agreeable to both the EU and the US. Companies which store confidential data belonging to third persons should review their current international data flow to ensure they are compliant.

Samantha Wilson
Associate

T: 0203 697 1906
M: 07780 221676
E: samantha.wilson@cpblaw.com