
## Commercial

# Data Shields for Transatlantic Transfers and Cybersecurity in the Post-Brexit Era

Negotiations between the EU and U.S. authorities regarding the security of EU citizens' personal data when it is transferred into the United States have recently concluded. Until recently the U.S. 'Safe Harbour' which had been approved by the European Commission was considered adequate to protect the privacy of EU citizens' data in transatlantic transfers. But in a landmark decision (*Max Schrems* case, October 2015), the European Court of Justice held that the U.S. Safe Harbour was inadequate to meet EU standards. Its replacement, the EU-U.S. Privacy Shield has now been launched.

The European Commission decides on a case-by-case basis whether a non-EU country has an "adequate level of protection" for data privacy. Pursuant to the 1995 EU Data Protection Directive, the Commission makes so-called 'adequacy decisions' regarding each country. The U.S. had adopted a Safe Harbour which the European Commission held in July 2000 to be adequate for ensuring the security of data transfers into the United States. However, the European Court of Justice invalidated this decision in the *Schrems* case. The rights of EU citizens to privacy were deemed insufficiently protected by the U.S. Safe Harbour. This also applies to countries such as China, Japan and South Korea.

*Privacy Shield*: Subsequent to the *Schrems* ruling the EU and U.S. authorities began negotiations to develop what is currently known as the EU-U.S. Privacy Shield. The Privacy Shield includes principles applying to U.S. businesses to ensure that EU citizens' personal data is adequately protected from unwanted disclosure. Also, in the United Kingdom, threats to the security of electronic data flows across international borders and the dangers of cyber-attacks have been highlighted as risks to be addressed by the efforts of British intelligence, administrative bodies and law enforcement agencies.

In November 2015 the UK Chancellor of the Exchequer announced that a National Cyber Security Centre (NCSC) would be established in 2016 and that £1.9 billion would be invested in cyber security over the subsequent 5 years. The UK Minister for Data Protection echoed the concerns expressed by the Chancellor in a July 2016 speech. She stressed the need for appropriate responses to technology failures and breaches which could erode the trust that individuals have placed in businesses, governments and data protection laws in the United Kingdom. This includes risks arising from misuse by hackers and losses of personal data which can cause great distress to individuals. The UK Minister also stated that businesses in all industries would need to focus on protections from cyber-attacks including commitments by managers to prevent, detect and respond to data privacy and systems security breaches. In addition she spoke of the need for training of all staff in order to increase awareness and improve the skills of employees for ensuring effective plans in case of attacks. With the NCSC set to open this autumn, this all indicates that data security and cyber safety continue to be considered high priorities by the post-Brexit UK Government.

*Contractual Protections*: EU standard contractual clauses (SCCs) and binding corporate rules (BCRs) are among the means by which businesses can ensure compliance with the data privacy standards of the UK Information Commissioner's Office. These have been approved by the ICO and the European Commission has also prepared model contracts for the transfer of personal data from the EU into non-EU countries.

In August 2016 the ICO issued a statement that use of the EU-U.S. Privacy Shield by businesses was recommended for data transfers outside the European Union. It also suggested that businesses use SCCs and BCRs in their commercial contracts.

*Contact us*: Should you require advice and assistance on compliance with the data privacy rules for transfers outside of the European Union or review of your commercial agreements for the appropriate contractual wording, please contact your usual 3HR consultant or Richard Hull, Commercial Solicitor at richard.hull@3hrcs.com.

**Richard Hull**
**Commercial Solicitor**
E: richard.hull@3hrcs.com