EU-US Privacy Shield

1 REPLACING SAFE HARBOUR

EU privacy legislation restricts the transfer and processing of EU citizens' personal data outside of European Union, unless the destination country was deemed to have in place adequate protection in line with that of the Union.

As a result of this, the Federal Trade Commission in the US negotiated a 'Safe Harbour' agreement with the EU. This agreement allowed exchanges of personal data between the EU and certain US companies, on the condition those companies agreed they could provide necessary protections when handing EU citizens' data.

In October 2015 the European Court of Justice (ECJ) ruled Safe Harbour was invalid and could not be relied upon to facilitate data transfers. The ECJ found the United States Security Services were able to access and gather EU citizen's personal data, and thus essentially ignore the terms of the arrangement. Similarly another criticism was that some US based companies were merely paying lip service to the data protection requirements of the agreement, and thus not properly adhering to the agreed data protection principles.

This finding by the ECJ led to frantic renegotiation between the US and EU. Larger businesses were generally able to adapt more quickly by adopting appropriate Data Transfer Agreements (through methods such as binding corporate rules or model clauses); however there was still a notable void left by Safe Harbour, which has recently been addressed by the implementation of the Privacy Shield.

2 PRIVACY SHIELD

The Privacy Shield aims to provide a set of robust and enforceable protections for the personal data of EU citizens. To enable such an agreement to take place the US Intelligence Services have provided assurances that any access to EU citizens personal data will be subject to clear limitations, safeguards and oversight. Any perceived infringements of these measures, or any complaints, will be investigated by an independent ombudsmen within the Department of State.

US based companies wishing to make use of the Privacy Shield arrangement will be placed in a register and required to annually self-certify they adhere to agreed data protection principles. These companies will have to be more transparent about how they adhere to privacy principles, who they share data with and provide information on their complaints procedure.

As well as being able to complain to the US Company registered to the scheme, EU citizens will also be able to take complaints to their own local Data Protection Authority who in turn engage the Department of Commerce or Federal Trade Commission in order to resolve a dispute.

3 IMPACT OF BREXIT

Guidance suggests the UK's expected withdrawal from the EU will mean the Privacy Shield would cease to have applicability to the UK. This is because is because it exists only as a mechanism for data transfer between the EU and US.

Commentators suggest it is unlikely a similar arrangement would not be negotiated by the UK prior to its exit from the Union. However if such an agreement is not agreed, UK companies would need to consider other robust methods of data transfer, perhaps through the use of binding corporate rules or model clause contracts.

4 FURTHER INFORMATION

Vero maintain an extensive library of documents relating to screening specific topics, including legislation and regulation. If you require further information on this or any other topic, please contact your Client Relationship Manager or get in touch via the 'contact us' page on our website.