# What impact does the EU-US Privacy Shield have for financial institutions engaged in litigation requiring the transfer of data from the EU to the US?

On Monday 1 August 2016 the EU-US Privacy Shield regime 'went live', replacing the Safe Harbour regime (which had been declared invalid by the European Court of Justice). Under the Privacy Shield regime personal data can be transferred from member states of the EU and the European Economic Area to specific entities in the United States which can certify themselves compliant with the Privacy Shield Principles (**"the Principles"**). However as we explain below this will have little, if any, impact on financial institutions faced with requests to transfer data from the EU to the US in connection with US litigation.

Before considering the Privacy Shield regime, we consider the processing of data in the EU before its transfer out to the US.

## Processing the data in the EU for the purposes of US litigation

The processing of personal data in EU member states is currently governed by the 1995 Data Protection Directive, as transposed into national law; in the UK this is achieved by the Data Protection Act 1998 (**"DPA"**). In order lawfully to process personal data, at least one condition specified in the DPA must be met. One condition that is often relied upon is that the processing is necessary for (amongst other things) the purposes of the EU company's legitimate interests (balanced with the interests of the data subject(s)), which would potentially include the litigation process.

Where data is sensitive personal data, at least one additional condition relevant to the processing of sensitive personal data must be satisfied. Normally the data subject's explicit consent would be required but sensitive personal data can also be processed where it is necessary to do so for the establishment, exercise or defence of legal claims.

Any personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not used for incompatible purposes. The personal data must be adequate, relevant and not excessive in relation to the purposes for which it is to be processed, in this case litigation.

This would require the EU company analysing how much of the information relevant to the case consists of personal data, and whether any of the personal data should be transferred in a redacted, anonymised or pseudonymised form, taking care always to balance the legitimate interest of engaging in the litigation process with the rights of the data subjects whose personal data is being processed.

## Transferring personal data

Other conditions have to be satisfied to transfer personal data from the EU or EEA. Normally under EU law personal data can only be transferred outside the EU or EEA if the recipient country ensures an adequate level of protection. The European Commission has identified only twelve countries that provide adequate protection, and the US is not one of these. It is possible for a transferring EU company to agree contractual provisions with the receiving US company based on EU model clauses, or, if a multinational group, to adopt so-called Binding Corporate Rules, but both of these regimes are subject to stringent conditions which make their applicability in the context of litigation problematic. There is an express derogation from the rules restricting transfer where the data is necessary for the establishment, exercise or defence of legal claims, necessity being strictly construed (in addition to the requirements for fair processing described earlier).

## Transferring data to a US company using the Privacy Shield regime

In order to use the Privacy Shield regime, the recipient US company must adhere to the Privacy Shield Principles (**"the Principles"**) and self-certify annually to the US Department of Commerce that it complies with them. The Privacy Shield regime is enforced by the US Federal Trade Commission (**"FTC"**) or the US Department of Transportation (**"DOT"**); therefore adherents to the Principles must already be subject to the jurisdiction of the FTC or the DOT in order to adhere to the Principles. This immediately limits the applicability of the regime. For example, entities such as financial institutions or law firms cannot adhere to the Principles and so cannot be subject to the regime.

The Principles are designed to protect not just the data but the rights of the data subject. For example the Principles require that the US company publish a notice detailing the extent and purposes of their data collection and processing. They also require that a data subject is given a choice as to whether their data is disclosed to a third party; and that all onward transfers of data are made pursuant to a contract which provides the same level of protection as the Principles. Therefore if the recipient US company adheres to the Principles (perhaps for information sharing purposes necessary to conduct its business), and receives personal data from the EU in that context, it will necessarily be restricted by those Principles as to how it processes the data, including in relation to transfers to third parties.

While it may be possible, subject to the requirements of fair processing, to transfer data for the purposes of review, there will clearly be significant issues in the context of disclosure to other parties in litigation where the relevant documents contain personal data.

## Conclusion

As banks and other financial institutions are not subject to the jurisdiction of the FTC or the DOT, they cannot adhere to the Principles – so they cannot take advantage of the Privacy Shield regime. Further, the very strict provisions regarding the handling of personal data under the Principles makes their application in the context of disclosure problematic.

For more information, please contact any of the following:

***Chris Roberts***
Senior Associate
+44 20 3130 3543
croberts@mayerbrown.com

***Ed Sautter***
Partner
+44 20 3130 3940
esautter@mayerbrown.com