SCOTTISHLEGALNEWS
News, Events and Jobs in Scottish Law

Blog: No port in a storm – the end for Safe Harbour?

Lindsay Urquhart *discusses the consequences for companies of the ECJ's Safe Harbour ruling.*

Lindsay Urquhart

The US government website http://export.gov/safeharbor/ where American companies can register to self-certify under the Safe Harbour scheme looks exactly the same today as it did before the Schrems decision, but the decision issued on 6 October 2015 has swept away the very foundations of that scheme invalidating EU-US data sharing arrangements founded upon it.

The US Department of Commerce reacted to the decision with the following comment: "We are deeply disappointed in today's decision from the European Court of Justice, which creates significant uncertainty for both U.S. and EU companies and consumers, and puts at risk the thriving transatlantic digital economy. Among other things, the decision does not credit the benefits to privacy and growth that have been afforded by this Framework over the last 15 years."

The American reaction is hardly surprising given that the CJEU decision is not a good news story, particularly for American companies who are now firmly shut out from the European Data Protection regime.

The decision will impact heavily upon all organisations that are structured around international data flows and sharing arrangements between the EU and the US. Snowden's revelations may have started the ball rolling by highlighting the vulnerability of data on US servers, but it is only now two years later that we are seeing the practical fall out.

Companies that use the Safe Harbour should take steps now to review their data transfer arrangements.

Wide reporting of the Schrem's decision and the involvement of Facebook are likely to ensure maximum publicity for the decision. Data Subjects will be well aware of the impact of this decision upon the processing of their data. This means they are more likely than ever to question where their data is stored and potentially report their concerns. National Data Protection Authorities now have a new mandate to investigate EU-US transfers and to question the decisions of the Commission.

These authorities will not, however, have any more resources in the short term with which to carry out that task, a factor which may restrict substantially their ability to enforce the European Court's decision.

These authorities will not, however, have any more resources in the short term with which to carry out that task, a factor which may restrict substantially their ability to enforce the European Court's decision.

The result is greater uncertainty with companies having to turn to alternative arrangements either in the form of self-certification of adequacy (a decision few data controllers will feel comfortable making), or placing reliance upon adequate safeguards. Adequate safeguards include the use of Standard Contractual Clauses or for larger organisations, Binding Corporate Rules approved by the European Commission for intra-group transfers. All of this will be costly and difficult for firms to implement.

As companies come under pressure to ensure their arrangements are adequate, they in turn are likely to place considerable pressure upon National Data Protection Authorities, who will respond with different approaches. The regulatory framework for data transfer will become considerably more difficult to navigate, representing a set-back for international trade and commerce.

The CJEU decision also raises the possibility of National Authorities questioning Commission decisions, raising the possibility of further scope for confusion and disagreement about national approaches to Data Protection Regulation.

- *Lindsay Urquhart is an associate at **bto Solicitors**, you can view her profile here.*