# Harbor Doubts — what the EU's 'Safe Harbors' decision really means

20 OCTOBER 2015

Kenneth Mullen
PARTNER | UK

**CATEGORY:**
ARTICLE

You may have read the headlines regarding the Court of Justice of the European Union (CJEU) decision in the Max Schrems v Irish Data Protection Commissioner case in which the 'Safe Harbors' Scheme for EU-US data transfers has been declared invalid under European law.

Some of the initial reaction seemed to verge on hysterical. The US tech industry is facing 'a legislative buzzsaw' or a 'bombshell'according to some sources and others seemed to indicate that the CJEU decision was a major threat to transatlantic trade. But is this really going to be the case?

As the dust settles, the following provides our brief reality check on the decision and what it means:

'Safe Harbor Certification' can no longer be relied upon to automatically legitimise EU-US data transfers. TRUE.

*US organisations that are subject to US Department of Commerce (DoC) jurisdiction can no longer rely on the automatic free-pass that the Safe Harbor gives them to receive EU data. There are 4480 US organisations with a 'current' certification who are directly impacted. Non-DoC regulated organisations who could never claim the benefit of Safe Harbors such as organisations in the banking, financial and charity sector are not directly affected. However, there is a wider, indirect impact on organisations that have been using the services of US affiliates, technology providers or data processors with Safe Harbor status. Generally if that EU client was sharing customer or employee data with a certified vendor (or its parent company) it had assurance that the data transfer to that US company automatically met data privacy requirements, without having to make further enquires. This is no longer the case.

Personal Data can no longer be legally transferred to the US and needs to be kept in the EU. FALSE.

*Some types of EU-US data transfers also automatically exempt (e.g. where a transfer is needed to obtain legal advice or necessary in order to perform a contract for an individual, such as reserving a US hotel), Furthermore, Safe Harbors was only one way to meet required EU Data Protection Directive standards. There are other routes to compliance – notably through getting an individual's freely given consent to the data transfer, use of the EU sanctioned standard 'model contract clauses' to cover the transfer, implementing binding corporate rules (for internal global transfers) or – certainly as far as UK organisations are concerned – data exporters can still make their own 'real-world' assessment of the US data importer's privacy/security arrangements and conclude that it meets required legal standards. On this last point, it's worth bearing in mind that organisations signed up to the Safe Harbors Framework have had to implement a range of privacy processes to be able to annually certify their standards under pain of DoC enforcement action. This is not a process that any of these organisations would have taken lightly, given that DoC sanctions are arguably a more fearsome prospect than the data privacy sanctions regimes of many EU authorities. This is on top of stringent State privacy legal requirements that some organisations have to deal with in places such as California. So practically – while alternative methods to legal compliance now need to be applied as a result of the CJEU judgment – privacy standards previously in place in formerly certified US organisations will not have suddenly disappeared.

US data importers are all about to be sued. FALSE

*First, as noted above the ruling only impacts on transfers to Safe Harbor registered companies. The judgment is an interpretative ruling and does not declare transfers to Safe Harbor registered companies as automatically illegal. It merely gives EU data protection authorities the scope to make their own judgment on legality. Yes, some high profile companies may now become targets for complaints by EU-based activists but claims that swathes of individuals/regulators are going to be taking enforcement action seem far-fetched.

As far as the UK regulator, the Information Commissioner is concerned, their reaction to the judgment recognises that affected organisations will need time to put alternative arrangements in place. The Article 29 Working Party of national EU Data Protection regulators has also issued a

similarly measured statement indicating that regulatory sanctions for data exporters are not imminent and, for the time being, model contract clauses and binding corporate rules will continue to be legitimate ways to comply with EU law. However there is a threat that if a solution is not found between US authorities and the EU by the end of January 2016, co-ordinated enforcement action is a possibility.

A new inter-governmental settlement seems to be the only logical long-term solution. An EU-US Umbrella Agreement for sharing of data in relation to law enforcement has just been finalised and it may well be that a successor to Safe Harbor may be round the corner on the back of this arrangement.

Summary

While some of the original reporting has been overblown, it would be a mistake to dismiss the Schrems judgment altogether. With the potential for increased scrutiny, all organisations exporting personal data between Europe and the US are now on notice that they should be reviewing their data transfer arrangements and policies.

- For EU or EEA companies exporting their data internally or externally – it is time to check contracts with US-based affiliates or data hosts/service providers and ask questions of those who have been relying on Safe Harbor registration as to what measures are now being put in place to deal with EU data privacy issues.
- For US data importers who are signed up to Safe Harbors, it is time to review customer contracts/privacy policies and look at alternative arrangements in order to give your EU associates and customers the assurance they need that you are on top of the issue.

Adopting an approach based on the EU model clauses would seem to be the obvious quick-fix for many businesses affected by the CJEU decision but each organisation should review its own individual situation, keeping an eye on EU developments, and take action.

# Authors


## Kenneth Mullen

PARTNER | LONDON

Intellectual property and technology

+44 20 7597 6189

kenneth.mullen@withersworldwide.com