MACFARLANES

HOW TO DEAL WITH THE EUROPEAN COURT'S SAFE HARBOUR DECISION

The confirmation by the European Court on Tuesday morning that the Safe Harbour Framework under which personal data that has been transferred from the EU to the US is now invalid has necessarily caused some concern about what steps should be taken next. This note answers some of the key questions:

1. IS THE INVALIDATION AUTOMATIC? IF SO, WHAT IS IN PLACE TODAY?

The European Court found that the Commission had exceeded its authority in entering into the Safe Harbour Framework Decision in 2000, so the working assumption must be that Safe Harbour is not in place today and has now disappeared. The EU Justice Commissioner, Věra Jourová, sidestepped the question at a press conference on Tuesday, instead stressing that discussions between the Commission and national Data Protection authorities were ongoing to decide on a unified reaction as to the right measures to be put in place to replace the former regime.

2. IF I HAVE PREVIOUSLY RELIED ON SAFE HARBOUR TO EXPORT PERSONAL DATA TO THE US, WHAT SHOULD I DO NOW?

There are three principal actions to consider:

2.1. Take the opportunity to assess whether all of the data transfers you are making to the US really are necessary. Are there other locations within the EU from which that same processing could be undertaken?

2.2. If you believe your data transfer model to be sound and that transfers to the US do remain necessary, consider whether you fall under any of the following exemptions:

- i. the data subject (the relevant individual) has given their unambiguous consent to the transfer;
- ii. the transfer is necessary for you to either (i) perform a contract between you and the data subject or (ii) take steps which the data subject has requested;
- iii. the transfer is necessary for you to conclude or perform a contract between you and a third party which is in the interests of the data subject;
- iv. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of a legal claim; or
- v. the transfer is necessary to protect the vital interests of the data subject.

2.3. If the transfers do not fall under one of the exemptions set out in 2.2 above, put in place the European Commission-approved standard contractual clauses (Model Clauses) for transfers outside the EEA as soon as practicable. This is a form of bilateral contract under which the relevant parties contract into providing the same data privacy protections as should otherwise exist under Safe Harbour. The form is available here and requires the addition of details of the specific transfers which are due to take place. The contracts do then have to be enforced and monitored as necessary, hence the concern about the extra (unnecessary) administrative burden caused by this decision.

3. ALL OF OUR EU EMPLOYEE DATA IS TRANSFERRED TO SERVERS HOSTED IN THE US WHERE OUR PARENT IS LOCATED. WHAT IS THE IMPACT OF THE DECISION ON THAT?

You may already have the consent of employees to such a transfer through your employment contracts. However for those with EU employees outside the UK, to the extent they are not already in place, consider putting Model Clauses in place to cover the transfer. This is because the notion of consent freely given within the employment dynamic is not universally accepted in the EU, and also because it is not easy to justify the underlying necessity of the transfer: you could as easily host such servers in the EU and still operate your business, even if such decentralisation may incur greater cost. The same applies for Customer Relationship Management and other commonly used enterprise databases.

4. IF ONE OF THESE "FIXES" WORKS, IS THAT ALL I HAVE TO DO?

Yes, although even a solution involving Model Clauses may be temporary. There is a second limb to the European Court's decision which is to recognise that the US government does not provide a means by which an EU citizen can take action against the NSA (as an arm of the US government) in the event that the NSA over-reaches its lawful surveillance powers. The US Congress is in the process of passing an amendment to federal law which would provide EU citizens the right to sue the US government. Until such time as this law is passed, even the Model Clauses route must be at risk, but pending any decision on that point, Model Clauses represent the most obvious means of resolving the problem.

5. WE DON'T HAVE ANY RELATIONSHIPS WHICH RELY ON SAFE HARBOUR. DOES THIS DECISION IMPACT ME AT ALL?

You may not have direct relationships which are reliant on the scheme, but do take the time to check your technology supply chain – do any of your IT vendors move your data between the EU and US for example? If so, what steps are they taking to deal with the issue? Even if a claim may seem remote, and the likely financial implications seem small, the reputational stain of being connected with a breach of the rules make the effort to confirm the point worthwhile.

6. WHAT RISK DOES THIS INVALIDATION CREATE?

There must only be a small liability risk to businesses which previously relied on Safe Harbour as a result of this ruling. A claim would need to be brought against you that a data transfer to the US was undertaken under circumstances which did not protect the claimant's rights and had caused loss/damage. The data protection authority (the ICO for the UK) would then have to assess the claim because you would naturally respond by saying that the data subject's rights were adequately safeguarded by virtue of the Safe Harbour Regime which was in place at the time. Since the national Data Protection authorities are meeting now with the European Commission to resolve the conundrum of maintaining data flows to the US, it would seem an unlikely result if they were to impose sanctions on a transferring party for adhering to a regime which they had hitherto supported. A due diligence defence of taking prompt steps to replace your existing data transfer regime system with, for example, Model Clauses or a re-assessment of the need for such transfers should be sufficient to rebut any claim based on data movement under the now invalidated framework.

CONTACT DETAILS

If you would like further information or specific advice please contact:

RUPERT CASEY
PARTNER
DATA PRIVACY
DD: +44 (0)20 7849 2256
rupert.casey@macfarlanes.com

OCTOBER 2015

MACFARLANES LLP
20 CURSITOR STREET LONDON EC4A 1LT
T: +44 (0)20 7831 9222 F: +44 (0)20 7831 9607 DX 138 Chancery Lane www.macfarlanes.com