TRENDING NOW

NOVEMBER 2015

LRN Inspiring Principled Performance℠

EU Court Ruling on Safe Harbour: What Now?

By Keith Read, November 2 2015

Miss part one of this story? **Read it here.**

Introduction

'Safe Harbour' - the agreement which allows transfer of personal data related to European citizens to the United States - has been a key backbone of the global data protection regime for the last fifteen years. However, in a case brought by an Austrian privacy activist following Edward Snowden's US National Security Agency (NSA) surveillance revelations, the European Court of Justice (ECJ) made a landmark ruling in early October 2015 which declared the agreement invalid.

This ruling has potentially significant consequences and, following a previous article which examined what the ruling means for companies both in the EU and US, we will now briefly consider what companies could, and should, do now.

What's the up-to-date position now following the ruling?

It has been widely quoted that some 4,500 companies previously utilized Safe Harbour, and are directly affected by the ruling.

EU law says that companies cannot transfer EU citizens' personal data to countries outside the EU which have insufficient privacy safeguards and, given the ruling, these 4,500 companies currently have no method of demonstrating compliance with EU privacy regulations when they transfer personal data to the US. Clearly, the European Commission (EC) and the US are under extensive pressure to agree a replacement system - with the EU Working Party on the Protection of Individuals now publicly stating three months as the target timescale. However, critics will say that the EU and US have previously worked unsuccessfully for some two years to reform the Safe Harbour agreement, with agreement proving elusive on the central issue of limiting access to personal data. Not surprisingly, the ruling has started to trigger a wave of requests to European data protection regulators to re-examine previously dismissed high-profile, household-name cases regarding the Safe Harbour system.

There are alternatives to Safe Harbour - such as 'model contract clauses' or Binding Corporate Rules - but these types of agreement are struck on an individual basis and require companies to guarantee that the transfer will be subject to an adequate level of data protection in accordance with EU standards and rules; given their practical

complexity, it is estimated that these agreements are presently used by less than 100 companies.

Following the ruling, companies face the risk of being prosecuted if they transfer the personal data of EU citizens to the US without effective privacy safeguards in place. However, in practice, regulators have now agreed on what is, essentially, a grace period until the end of January 2016 - in line with the three-month timescale above.

What should companies do now?

Whilst a replacement to Safe Harbour is being agreed - and the reports are that progress is being made - companies need to recognize, and consider, where Safe Harbour data privacy impacts their activities; clearly, the impact may not just be confined to customer data and there may also be consequences for operations, internal investigations and litigation.

However, companies now have the opportunity to utilize this interregnum to their advantage and, for example, to:

Raise the profile of effective international data protection with affected employees*:*

Whilst many companies do have regular data protection and/or information retention training in place, this can sometimes by perceived by employees as a 'box-ticking' exercise. The opportunity now is to really drive home the potential risks and consequences of data protection issues and failures, using focused communications coupled with leading-edge training.

Identify hitherto hidden and masked data processing and protection issues:

Companies often unnecessarily expose themselves to data protection risks and failures by simply not fully understanding what data they currently have, what they are processing and where it is stored. A data protection review will make a company significantly better able to comply with new and existing legislation and standards, both EU and internationally

Deploy determined data culling to minimize data collection, transfer and associated risk*:*

Clearly, companies may not know in advance what data they need for a particular activity, development or investigation. However, once they have that basic understanding, then the opportunity is to minimize data collection and transfer - which

brings with it a host of benefits including data privacy compliance, reduced document review and reduced costs

Refresh and renew data protection, data security and information retention processes:

Whatever form the replacement of Safe Harbour finally takes, it is clear that the requirement for effective data security, for example - both physical and otherwise - will not be reduced.

This security requirement does not end at the 'factory gate' and, more than ever, will extend to a company's third-parties. Regular training, audits and implementation of recognized standards are central to comprehensive data security, as is avoiding the 'usual suspects' - such as lost and compromised laptops and USB sticks.

Leverage new and existing EU partner relationships for data hosting and processing:

Why move data outside the EU when it doesn't need to be? This simple option may not always be feasible, but companies can often succumb to transferring data internationally without a compelling reason, nor full recognition of the associated risk.

The current Safe Harbour issue may bring with it the opportunity for companies to - genuinely - examine why they transfer EU data to the US.

Summary

Concerns about Safe Harbour are certainly not new and the ECJ ruling was not entirely a surprise. As a consequence, the largest companies have had enough advance warning to prepare - but the widely-held view is that it is companies outside this 'top-tier' who will face the biggest challenge to prepare.

Notwithstanding the three-month/January 2016 Safe Harbour replacement timescale, above, it will take some months beyond that for the finer points of an agreement to be concluded; in the meantime, the companies that focus on data protection best practice will be those who emerge better-placed to deal with an environment of unquestionably tougher regulation and greater public focus.