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.

Risky Business? When a New Acquisition Brings More than You Bargained For

By Susan Divers, November 9 2015

Mergers and acquisitions are a major source and opportunity for growth for many companies, but while the business teams are popping champagne corks to celebrate the deal, the ethics and compliance team may be reaching for the Ibuprofen.

As the Department of Justice and Securities & Exchange Commission's 2012 Guide to the Foreign Corrupt Practices Act states—

Companies acquire a host of liabilities when they merge with or acquire another company, including those arising out of contracts, torts, regulations, and statutes…including those arising under the FCPA.

The risk of acquiring a major "landmine" in the form of past or ongoing FCPA violations is real, particularly if the target company has not been subject to the FCPA beforehand. When an FCPA "landmine" explodes after the acquisition or merger closes, it can have a severe financial impact on the acquirer, even if the improper conduct has stopped.

Consider RAE Systems. Headquartered in San Jose, California, RAE makes chemical and radiation sensors and monitoring systems. According to the DOJ, the company did business in China from 2005 to 2008 through two subsidiaries, RAE-KLH and RAE-Fushun. Customers included Chinese government departments, state-owned businesses, regional fire departments and other semi-governmental bodies. RAE did due diligence before acquiring a majority stake in the joint venture that became RAE-KLH and became aware of improper commissions and kickbacks, yet the internal controls the company implemented only went "halfway," and the problem payments continued. Similar corruption indicators cropped up when RAE took control of the joint venture that became RAE Fushun but this time, RAE did no due diligence on pre-acquisition corruption. RAE then failed to put effective controls in place, according to the DOJ, or account for improper payments in its books and records, according to the SEC.

The company ultimately paid a $1.7 million fine and disgorged $1 million in profits from the illegal activity predating the acquisition. The SEC routinely requires such disgorgement as part of a settlement, even if the illegal activity has stopped after the acquisition closes. That can blow apart the financial underpinnings for the transaction.

What are some practical steps to take to avoid M & A landmines, whether they are FCPA violations or other problems?

Here are some best practices:

1. A thorough due diligence from a reputable provider before the M & A effort gets underway can save money, time and regret later on. If the target has a reputation for unethical practices or is on the regulators' radar, the acquirer should assess the risks, the effort and the cost of dealing with potential problems and/or remediating them before going ahead.

2. Ethics & Compliance needs to be a full partner on the due diligence team for an acquisition, merger or joint venture formation, not merely a recipient of limited data.

3. Make sure E & C attends due diligence discussions with the marketing teams, not just the legal or corporate staff. Marketing discussions give good insights into how a target gets business and keeps it and the extent it deals with government officials.

4. Internal audit should participate and review the target's internal controls. A target with lax petty cash controls, weak reconciliation practices and opaque accounts is a target that will need substantial overhaul and controls when a deal closes. Providing Internal Audit with a chance to familiarize themselves with the company gives them a leg up on what needs to be done.

Okay, we own it, now what?

Once an acquisition closes, the work of the E & C team becomes even more critical. Integrating a company that was never subject to public disclosures, securities laws and internal controls takes work and planning. Helping new colleagues understand Sarbanes Oxley, conflicts of interest, FCPA, sanctions and the host of new laws and regulations is the first step.

LRN recommends Code of Conduct training as soon as practical after an acquisition closes, to welcome new colleagues into the culture and set expectations. Proactive, 100% participation Code training on the heels of closing sends a strong signal about values and helps prevent resistance to new practices from building up. LRN's team can help update a Code to make sure it communicates broadly and effectively the partner's values and is translated into necessary languages.

Integrating an acquisition successfully is a long term project.

Here are some other best practices:

1. Setting out a project plan with key objectives for integration and responsibility and a timetable for meeting them promotes accountability and prevents risk areas from falling off the radar.

2. Analyzing the risk profile of the acquired company and tailoring a suite of training materials to rapidly bring them up to speed on key areas is also prudent. For example, strong internal controls are a key element of SOX and FCPA compliance as well as good business practice. LRN's library includes resources on FCPA, conflicts of interest and financial integrity, including the Speaking Up and Financial Reporting Vignette. Combined with in person training, this helps establish relationships and clarify expectations at the outset.

3. Working in partnership with Internal Audit, the E & C team should identify the key areas for strengthening or remediation of the acquired company's compliance. Scheduling an audit for six months after closing, in which the E & C team participates, helps set a timeframe for implementing changes and an incentive to get them done.

4. Developing a regular communication plan that involves senior managers, middle managers and regular events focused on values and speaking up is an essential element for success. LRN Advisory Services can help structure one that works and promotes cultural integration.

5. Coaching the acquired company's management on values-based leadership will help ensure that ethics and compliance is internalized into behavior, not merely a set of rules. LRN's GCLA team is highly experienced in this area.

Avoiding Corporate Catastrophes: Do You Know Who Your Business Partners Really Are?

By Susan Divers, Nov 16 2015

Several years ago a successful US high tech company was approached by a South American bank to upgrade the bank's information technology system. Contract negotiations went well and the estimated profit margin was over 20%. At the last moment, however, the company's due diligence revealed that the bank's major shareholders had associations with drug cartels. Further research turned up more (not less) red flags. The US company terminated negotiations. Improving IT systems that were probably handling drug money wasn't consistent with its values or compliance program.

Recently, a worldwide engineering firm preparing to bid on a high speed rail project in Russia met with the government entity preparing to issue the RFP. The officials let it be known that certain local subcontractors had been pre-approved and hinted strongly that teaming with them would enhance the chance of winning. Due diligence on the preferred subcontractors showed they were both recently incorporated in the Cayman Islands. The CEO of one was a former fashion model with no technical or corporate experience. When asked for further information about their shareholders and expertise, neither company provided any relevant information. The engineering firm declined the team, recognizing that there were significant corruption red flags and a lack of transparency.

Knowing your business partner is a major aid to avoiding ethical, business, legal and regulatory problems as well as fraud or other catastrophes.

Of course not every sub consultant, vendor, partner or business associate can be fully vetted through extensive due diligence, but identifying those that pose the highest risk or present red flags can allow companies to target their due diligence efforts effectively.