FRA Insight: A Change In Attitudes To Digital Data

Don't Get Caught Out By The Latest Changes To Digital Data Privacy And Disclosure Laws

Reactions inspired by the Snowden leaks continue to heat up, the most recent being Roussef's plans set up Brazil's own secure email servers and to introduce legislation that would require all online information concerning Brazilians to be stored physically in Brazil. What is clear is that there is a significant gulf between the US attitude towards data flows and data protection and that of the rest of the world. There have long been conflicts of law but with the importance of the Internet, the promise (and threat) of Big Data and the proliferation of data volumes, life is just going to get more complicated, particularly if you are a corporate operating internationally.

The proposed new EU data protection regulation, if it passes, is set to increase privacy rights and by extension costs related to compliance. However, in the wake of the NSA leak scandal, regardless of whether that regulation passes or whether other jurisdictions introduce data protection laws, for political or sovereignty reasons more restrictions, enforcement and penalties surrounding data protection are inevitable. This will have significant implications for how and where companies choose (or are permitted) to store their data and whether they choose to outsource it. After all, does a third party, care as much about your data – and your legal obligations (which may be very complicated if they span several jurisdictions) as you do – and can they keep it safe – from the US government, enforcement agencies, industrial espionage, cyber threats, etc.?

The trend for cost saving purposes has been to outsource to third party data handlers such as Cloud providers or, in the event of a US driven dispute, eDiscovery vendors. We expect that trend to be reassessed by the risk aware corporate and for the demand for nuanced, expert and forward thinking advice on how to combat data loss and non-compliance with relevant data protection laws to increase. Corporates will need to seek out advisors who can think globally – and with cultural sensitivity – in a non-US centric fashion. Further, we expect where, how and why international companies keep different types of data – and how that is protected – to become a matter of business strategy as well as security and compliance.

Still Got Your Head In The Cloud?

A rule of thumb, when it comes to data storage is that the data is subject to the laws of the jurisdiction in which it is stored. Cloud computing has provided an avenue for storing troves of personal and private data online. An issue of key importance is the jurisdiction where a cloud provider is physically storing data. This couldn't be more apparent with the recent revelation of the US's National Security Administration (NSA) highlighted by press leaks which revealed that the organization has been gathering and storing metadata from Verizon and nine other US based Internet communication companies. These recent NSA revelations came as a surprise to some, in particular those who assumed they were protected by the US's fourth amendment (where there is a reasonable expectation of privacy). However, once information is shared with a third party (i.e., cloud provider) the expectation of privacy could likely be forfeited.

In response to this recent concerning news, European nations are tightening up data privacy laws to protect the personal data of their citizens, specifically with regard to potential US exposure. For example, the Norwegian government has banned the use of Google Docs in various cases, particularly where personal data are concerned and the Danish authority has banned its use where sensitive data are concerned.

France's CNIL (The Commission Nationale de l'informatique et des Libertes), an organization that is well respected in the subject of data protection, has published recommendations for companies using services offered by cloud providers and has highlighted potential risks presented by the US. CNIL states that the risk of foreign authorities accessing data, e.g. under the Patriot Act in the United States, must be taken into account in any risk assessment. Neelie Kroes, the European Commissioner for Digital Affairs, quoted in the Guardian, A UK National Newspaper, said, "If European cloud customers cannot trust the United States government, then maybe they won't trust US cloud providers either."

Digital Data, Physical Borders

There are general guidelines that companies should follow when considering cloud providers. However, particular concern should be paid to the physical location of a company's data. Find out where your cloud provider stores live data as well as backs up copies of your data (they all make copies of client data to maintain 24/7 access and to offer service level guarantees). Ask for the backups they make of your data to be stored in the same location you specified for your original data and applications.

It is strongly recommended that high-risk data – such as financial, corporate and personnel related data is always hosted in its jurisdiction of origin or one that carries similar protections. Emails are often highly sensitive in EU jurisdictions and carry strong data privacy rights, which makes transmitting or producing them outside of their jurisdiction of origin, not just risky, but potentially illegal. So, if a location-based guarantee from your cloud provider isn't possible, then think very carefully about that data and applications you put into a cloud environment – and carry out a full risk assessment.

This advice holds true when embarking on a cross border regulatory investigation with a team of external eDiscovery service providers. Find out where your eDiscovery service provider needs to physically store data for processing. Keep in mind that most mainstream eDiscovery providers maintain large data centers in the US and as such need to transfer data there (sometimes illegally) to accomplish their task.

For more information, please visit www.forensicrisk.com

Contacting FRA

FRA's offices are located in the US and in Europe and we have datacenters in each country of operation, to ensure compliance with local data protection legislation.

London, UK: +44 (0)20 7 831 9110

Switzerland: +44 (0)7747 790 232

Paris, France: +33 1 53 43 62 61

Washington DC, USA: +1 (202) 709 7475

Providence RI, USA: +1 (401) 289 0866