KASALANA
Global. Ethical. Intelligent.

UK: 0844 593 0230
Intl: +(44) 1580 212 832
E: info@kasalana.com

Our Perspective

Safe Harbour invalidation: is data localisation inevitable?

On 6 October 2015, the *European Court of Justice* (*ECJ*) ruled that the Safe Harbour Decision is invalid as it does not offer adequate data protection.

To receive regular issues of Kasalana's Our Perspective updates, please email anna.goddard@kasalana.com quoting reference OP10

The Safe Harbour framework allows personal data to be transferred from EU countries to the United States. US companies self-certify that they uphold certain standards protecting personal data and their certification is kept on a register held by the US *Department of Commerce*.

Thousands of companies use this framework to approve the transfer of data between the two jurisdictions, but the future of transfers approved on this basis is now in question.

The implications of the ruling

The consequences of the ruling are potentially disruptive and expensive. Large companies such as *Google*, *Facebook* and *Amazon* are undoubtedly reviewing their data transfer and storage processes. Many of them, as evidenced in the case of *Schrems v Data Protection Commissioner* that brought about the invalidity ruling, routinely move personal data outside the EU to servers kept in the USA, where Safe Harbour self-certification does not apply to public authorities and can be overridden by national security requirements. These requirements allow US authorities to access data for purposes other than those for which it was originally intended.

Anecdotal evidence suggests that, in the longer term, large multinational companies will have to localise their data by building data farms within the confines of the EU. *Microsoft* has already taken it one step further through a legal arrangement with *Deutsche Telekom* which places EU data firmly out of the reach of the US Government.

Is the cloud the answer?

According to *Patrick Salyer* of www.computing.co.uk:

"For smaller and non-tech companies, on-premises storage and management of consumer data in several regions will be either not feasible or extremely cost-prohibitive."

He goes on to point out that there is nevertheless an opportunity for these smaller international enterprises to move their data from on-site owned data centres to one of the many international cloud-based data systems. Such service providers are already gaining popularity with growing businesses because of their relatively low cost and scaleability. They have more money and resources, and are already putting into place new and more adequate infrastructures and processes to safeguard personal data during international transfers. For those considering cloud-based solutions, the UK *Information Commissioner's Office* publishes a very useful checklist in their *Guidance on the use of cloud computing.*

But what of those small businesses in the EU already using cloud-based software and services from US companies who routinely transfer this data outside the EU to their servers based in the US? *Computer Weekly* reported that binding corporate rules (used for intra-group data transfer) and model clauses (for use between data exporters and data importers) could both help meet the adequacy standards of EU data protection laws. But it also questions the practicality of such clauses where a supplier has thousands of customers based in the EU.

EU GDPR and the US Department of Commerce

The *European Commission* has been negotiating a new Safe Harbour agreement with the US since the Snowden revelations two years ago. These negotiations could be the answer to ensure that US services to EU companies continue uninterrupted. However some feel that the recent *ECJ* ruling could hinder rather than bolster these negotiations.

The *European Commission* has also been discussing new General Data Protection Regulations (GDPR) with member states since it first proposed them in January 2012.

On 15 December 2015 the *European Parliament*, the *Council* and the *Commission* reached agreement on these rules. Further information can be found at ec.europa.eu. *Felix Braz*, justice minister for Luxembourg, commented:

"This reform not only strengthens the rights of citizens, but also adapts the rules to the digital age for companies, whilst reducing the administrative burden."

Conclusion

The sudden disappearance of the Safe Harbour framework will have left many companies reeling, and its implications are not yet completely understood. However, it is clear that consumers in this digital era are more savvy and careful than ever before, and enterprises must now address the evolving issues and potential pitfalls of international data transfer before they arise.

The onus is now on the *European Commission* and national *Data Protection Authorities* to guide businesses on what they need to do to ensure that their data storage and transfer comply with the law.

Why we do what we do

At *Kasalana* we have a client-centric approach to intelligence and believe in giving our clients what they need. The information we supply is openly asked for and freely given, and all our work is overseen by senior consultants with many years' experience in their field. With an ethical approach to investigation, we support improvements in global business practices and security.

All our intelligence is individually sourced and produced at the time of commissioning to answer the specific needs of our clients. We work honestly and transparently using a global network of resources to provide timely and accurate information to international clients. To read case studies, please go to www.kasalana.com.

Consultation meetings

If you would like a free consultation with *Kasalana*, please email info@kasalana.com quoting reference OP10C.

Who we are

Formed in 2005, Kasalana is a specialist corporate intelligence company that conducts investigations globally on behalf of clients from industries including automotive, aviation, construction, consumer products, defence, energy, engineering, financial services, insurance, legal, manufacturing, media, medical, mining, professional services, retail, technology and telecommunications. We are experts in enhanced due diligence, background checks and legal support services including asset tracing & litigation support, corporate fraud investigations, merger & acquisition support and strategic & market intelligence. Our clients include FTSE-100, FTSE-250 and Fortune 500 corporations, global financial institutions, major law firms and leading private equity houses.

Prior to forming Kasalana Sam Pope was Head of Business Intelligence, Deputy Director of Corporate Investigations and EMEA Director of Fraud & Forensic Services for a leading global security risk management company, where he led a team of 40+ investigators. A former defence journalist, Sam has extensive experience of investigating fraudulent activity including asset misappropriation, bribery and corruption, intellectual property fraud, false accounting, securities and investment fraud, regulatory and anti-trust violations. He frequently works in close collaboration with clients' other professional advisers. He is a member of the *American Society for Industrial Security* and the *Association of Certified Fraud Examiners.*

Gareth Crooker joined Kasalana in 2010 after working as Director of Corporate Investigations, South-East Asia, for a leading global security risk management company. He has been a business risk consultant for more than 20 years and specialises in pre-investment and compliance-driven due diligence and business intelligence. Gareth has also conducted bespoke research and analysis into the political, commercial and security risk environment in Europe and the Former Soviet Union. As well as his native English, Gareth has near-fluent French and Spanish, together with basic Italian and Dutch.