GIR Global Investigations Review

Avoiding data protection pitfalls: Spotlight on cross-border investigations

7 January 2016

Credit: Thijs ter Haar on Flickr (CC BY 2.0)

The EU's recent decision to abandon its 15-year-old Safe Harbour rules covering data transfers to the US is likely to cause major headaches for lawyers carrying out internal investigations. **Toby Duthie** at Forensic Risk Alliance and **Simon Taylor** at Weil Gotshal & Manges explain why.

On 6 October, 2015, the European Court of Justice (ECJ) issued a game-changing and non-appealable ruling in *Schrems v Data Protection Commissioner* invalidating the European Commission's decision, which had stood since 2000, that the data privacy principles of US-EU Safe Harbour provide an adequate level of protection for the data of EU citizens.

Safe-Harbour principles can no longer be relied on and the data protection commissioner (or equivalent) in each EU member state can now question whether transfers of personal data to the US comply with EU data protection law and to suspend such transfers if EU privacy obligations are not met.

The impact is potentially enormous for the thousands of US multinational companies that operate under Safe Harbour (as well as for the thousands of European businesses that have their data hosted in the US by these US companies). While the European Commission has indicated that it is committed to finding a "safer" safe harbour, so that the transfer of transatlantic data can continue, this is likely to take some time. For now, companies that rely on the US-EU Safe Harbour agreement must review their current practices and consider alternatives.

This article considers the specific implications of this decision on corporate internal investigations and offers practical suggestions as to what companies should be doing to operate within the law on data privacy as it currently stands.

First published on the Global Investigations Review website, 7 January 2016
globalinvestigationsreview.com

GIR Global Investigations Review

Context: Snowden's whistleblowing and the NSA's PRISM programme

Maximilian Schrems is an Austrian national residing in Austria. He was a Facebook user. From 2008 he had a subscriber agreement with Facebook Ireland Ltd. Facebook Ireland kept its subscribers' personal data on servers located in the US.

In the light of the revelations made by Edward Snowden (from May 2013) that, under a programme known as PRISM, the US National Security Agency (NSA) obtained unrestricted and undifferentiated access to mass data stored on servers in the US owned or controlled by a number of companies active in the internet and technology sector, Schrems made a complaint that the US-EU Safe Harbour principles did not, in fact, contain adequate safeguards for EU citizens under EU data privacy laws.

The Irish data protection commissioner refused to investigate his complaint on the grounds that it was unsustainable in law. When Schrems sought a judicial review of that decision, the High Court referred the question to the Court of Justice of the European Union (CJEU) for a ruling. On 23 September, 2015 Advocate-General Bot ruled in favour of Schrems and, just two weeks later, the full CJEU confirmed it.

What is personal data?

To understand the impact of this decision upon corporate internal investigations, it is important to be clear on what amounts to "personal data" for the purposes of the protections provided by EU law. EU directive 95/46 defines personal data as any information relating to an identified or identifiable natural person. An identifiable natural person includes one who can be identified directly or indirectly. This includes identification by reference to specific physical, physiological, mental, economic, cultural or social factors. It is, by any measure, a broad and embracing concept intended to extend well beyond what would be regarded as personal information in an everyday context. The courts have attempted, on a number of occasions, to give guidance on the application of the test in the directive.

At the EU level, in criminal proceedings against Bodil Lindqvist, the CJEU stated the term "personal data" covers information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone co-ordinates or information about his working condition or hobbies. In *Commission v Bavarian Lager*, the court stated that the definition of the concept of single personal data correctly held that surnames and forenames may be regarded as personal data.

In the UK there have been a string of cases from 2003 refining the approach. Most recently, Lord Justice Moses in *Efifiom Edem v Information Commissioner and Financial Services Authority* gave the following guidance:

"It is important to remember that it is not always necessary to consider 'biographical significance' to determine whether data is personal data. In many cases data may be personal data simply because its content is such that it is 'obviously about' an individual. Alternatively, data may be personal data because it is clearly 'linked to' an individual because it is about his activities and is processed for the purpose of determining or influencing the way in which that person is treated. You need to consider 'biographical significance' only where information is not 'obviously about' an individual or clearly 'linked to' him."

What is 'Safe Harbour'?

European data privacy law prohibits the transfer of personal data to a country outside the European Economic Area unless that country ensures an adequate level of protection for individuals' personal data. The Safe Harbour programme was established in 2000 to enable US organisations to comply with European law. The US Department of Commerce worked with the European Commission to develop a "Safe Harbour" framework, which allowed US organisations that self-certified compliance with the Safe Harbour principles (which are similar to EU data protection principles) to transfer data concerning EU citizens.

GIR Global Investigations Review

What does this mean for internal investigations?

The recent memo from US Deputy Attorney General Sally Yates (the Yates Memo) is a stark reminder to corporates that, if they wish to achieve full credit for cooperation, internal investigations must be conducted thoroughly into suspected wrongdoing and must focus from the outset on the conduct of individuals.

The first step in any internal investigation is fact gathering. This will always involve the collection, transfer and processing of data about the conduct of individuals in the organisation. This necessarily involves manipulating, analysing and moving vast quantities of personal data. For any businesses with operations in the EU this will inevitably put that process in conflict with EU privacy laws. The end of Safe Harbour will pose very real difficulties for corporates to remain within the boundaries of EU law.

Previously, under the Safe Harbour framework, US companies frequently either self-certified compliance or used third-party forensic data vendors, lawyers or accountants with Safe Harbour certification to enable data to be transferred to the US for processing and analysis. Even under the now-defunct Safe Harbour regime many advisers and firms were still concerned that this was not sufficiently robust due to the very nature of any self-certification process and because certain EU national statutes, such as the French Blocking Statute, in a potential litigation context conflict with any Safe Harbour provisions. However, in reality, many did rely on Safe Harbour nonetheless. This is no longer an option (however misguided it may have been).

Building on the Yates Memo, in November 2015, Assistant Attorney General Leslie Caldwell took the opportunity to emphasise that companies will be expected to demonstrate that they "acted promptly" to deal with an FCPA violation and conducted "thorough and tailored" internal investigations. It is clearly important that companies quickly develop practical solutions to the obstacle created by the Schrems decision. Earlier, in May 2015, Caldwell made the following remarks about companies that rely on foreign data privacy laws:

"We recognize that some foreign data privacy laws may limit or prohibit the disclosure of certain types of data or information. Over the years, the criminal division has developed an understanding of certain oft-cited data privacy laws, and we will challenge what we perceive to be unfounded reliance on these laws to justify withholding requested information."

It will clearly not be open to companies to use Schrems as an excuse for being unable to conduct effective investigations or to withhold documents from the Department of Justice.

What are the post-Schrems options?

There are a limited number of short-term options, most of which come with disadvantages and cost implications.

1) Corporates that are affected need to restructure data storage architecture to ensure that European data remains in Europe. This will add significant costs and may also affect corporate structure. This does, however, ensure that no breaches of EU privacy laws occur in the normal trading activity.
2) For the transfer of data during an investigation, the obtaining of specific informed consent from the individual is theoretically possible, but undesirable. True informed consent is difficult to justify ex post facto to a data commissioner, particularly when US corporates are now on notice, post-Yates Memo, to target culpable individuals. Equally, tipping an employee off as to the existence and scope of an investigation may be counterproductive in the early phases of an investigation.
3) Adopting binding corporate rules (BCRs), which are internal rules adopted by multinational groups of companies and approved by the EU. BCRs can be costly and time consuming to develop and implement, but would provide a US company with essentially the same capacity to transfer data as it enjoyed under the Safe Harbour agreement.
4) Adopting the pro forma model contractual clauses approved by the European Commission. This may not be effective on a retrospective basis and therefore may not cover historic data that could be needed for investigatory purposes.

First published on the Global Investigations Review website, 7 January 2016
globalinvestigationsreview.com

5) Ensure that data is collected, processed and analysed in Europe and not transferred to the US. Clearly, this will provide peace of mind but will involve additional costs to ensure that the teams of forensic and legal specialists can be available in the relevant jurisdiction. Further considerations will also come into play in the event that the company wishes to self-report to the DoJ or provide documents containing personal data to the DoJ. It may be that the exception to the normal prohibition can be employed in these circumstances, allowing a company to transfer data where it is necessary to defend or establish its legal rights.
6) Conduct vendor due diligence to avoid vicarious third-party liability. In many cases, companies being fined are often at fault for the actions of their vendors – it is therefore important to employ vendors that comply with any relevant legislation, and have the capabilities to implement robust and secure in-country solutions. Experienced vendors will work at the outset with the company's legal team to adopt the most appropriate approach to data transfers.
7) One increasingly popular solution is to employ a vendor with the ability to deploy a mobile processing and hosting solution. In situations where there are regulatory or commercial sensitivities (eg, the data cannot leave the specific jurisdiction, or even the client's premises), a mobile solution can work to satisfy any such restrictions. In most cases, vendors that offer such unique products will be able to tailor the solution to the client's circumstances and requirements – the amount of data that needs to be processed, the accessibility options, the IT infrastructure, and any forensics work that needs to be carried out. The mobile solution can be in the form of a laptop, desktop or a server, and will be pre-loaded with customised hardware and software to handle the data and the investigation requirements, as well as will come with specific access limitations (eg, it will be limited to the IP address of the reviewer, and all other connections will be blocked). Further, the reviewer will only be allowed to carry out tasks that are pre-agreed, and any other work, such as managing software or hardware, will be dealt with by the vendor's engineers on the client's premises.
8) If in doubt, it is prudent to seek advice from the European data protection legal specialists. The EU regulators have said that they will not take coordinated action until the end of January 2016, which gives the companies time to seek expert advice. The risks at stake are high - those in violation of the current data protection regime companies stand to face regulatory enforcement, as well as potential legal action by both their customers and employees. EU data specialists will be able to advise companies on their data movement strategies, as well as conduct expert risk assessments of such issues as data being transferred through third parties, leaving the company liable in the eyes of the law.
9) Stay patient and vigilant. Safe Harbour 2.0 has been promised by the European Commission. However, the reasons underpinning its revocation were largely political rather than technical. Structuring Safe Harbour 2.0 is therefore likely to take time and, until it is agreed and introduced, companies will largely have to deal with the European data protection agencies. It is thus crucial to stay vigilant as to the applicable rules in each jurisdiction. In reality, however, will Safe Harbour 2.0 ever fully address contentious situations, especially those in which corporate and individual interests may sharply diverge? It is important to consider that Safe Harbour was only ever intended to assist companies manage data in their everyday business. It is also interesting that Microsoft recently announced that it will be opening Germany-based data centres that will be run by Deutsche Telekom as "trustees". This speaks volumes as to the challenges that Safe Harbour 2.0 negotiators face and to which businesses will very likely respond in the near term by building decentralised non-US IT infrastructure. This may, perhaps paradoxically, undermine the need for a treaty.
10) Conduct an assessment of the company's readiness for the EU Data Protection reform, a deal which was struck on 15 December 2015. The reform aims to give customers increased control over their data, its usage and retention, and will be implemented by all 28 member states passing uniform national legislation. It is important for companies to conduct self-assessments and to understand the potential implications, as the new rules will save compliant companies an estimated €2.3 billion per year – as well as impose fines of 4 per cent of global revenues for non-compliance.

First published on the Global Investigations Review website, 7 January 2016
globalinvestigationsreview.com

Finally, it's worth noting that post-Snowden concerns are not unique to the EU. A huge number of other countries including Brazil, Russia, China and Indonesia have introduced and enhanced data protection legislation. It seems clear that the legislative data protection-related tensions between jurisdictions – notably with the US on one end of the spectrum and the EU on the other – is only likely to grow. Data protection has morphed in the past couple of years into a major issue that requires consideration in the investigative context from the outset. Further, there is clearly political will to enforce breaches and EU penalty levels could potentially compete with those seen in the context of, for example, antitrust, sanctions and FCPA.

First published on the Global Investigations Review website, 7 January 2016
globalinvestigationsreview.com