European Court rules Safe Harbor invalid in Schrems case

Date : November 19, 2015

Originally published on 6th October 2015

[19.11.2015] We're trying to keep this primary article on this very important development up to date so that it can be your reference point for all things Schrems during this fast moving period. Updates from the original article are in bold and prefaced with the date of the update, and may contain links to other, more detailed, alerts we have issued on the development in question.

Overview

Today, following the recent Opinion of the Advocate-General in the very important European Court Schrems case (background below) which we previously reported on including in a video here and a podcast here, the judges gave their judgment in which they have largely followed the Advocate-General's Opinion and ruled that:

- The EU Safe Harbor regime is invalid; and,
- National EU Member State data protection regulators *do* have the independent power to investigate complaints about the adequacy of the level of protection of data transfers to the US and to suspend data transfers if they conclude that the US (or indeed any other jurisdiction outside the EEA) does not provide an adequate level of protection.

Outcomes & Comments

1. The immediate and direct consequence of the judgment is that the case will go back to the Irish High Court which referred it, and the Irish data protection regulator is required to examine Schrems' complaint swiftly and decide whether, under EU Data Protection Directive 95/46, the transfer of the data of Facebook's European subscribers to the US should be suspended on the ground that the US does not afford an adequate level of protection of personal data. The Irish regulator has already announced that they will be addressing this matter as quickly as possible.
2. The Safe Harbor regime no longer acts as a blanket exemption to the prohibition on transferring data outside the EEA or jurisdictions adduced by the Commission to provide adequate protection of data (in the words of the directive to "third countries").
3. Individual data protection authorities are given more power to investigate the adequacy of the protection of data in third countries, and to suspend transfers to those countries if they find them lacking – even if there has been a European Commission Decision to the contrary. **[20.10.2015] Indeed, one authority, of Schleswig-Holstein in Germany, has spoken out indicating that there are few solutions to sending data to the US.** For more information see our report here.

So what do we do?

Right now:

1. Work on a plan. The court's decision didn't give a transition period, and so it appears to take effect immediately. However, the Commission and most of the data protection authorities across Europe have acknowledged already that it will take time for businesses to resolve this, and indeed that the authorities need to get their heads together to address how they are going to deal with it, with support from the commission and the Article 29 Working Party. [19.10.2015] The Article 29 Working Party have confirmed that transfers under Safe Harbor since 6 October are unlawful, and that other provision must be made to protect personal data. For more information, read our report here. **[03.11.15] However as we've said elsewhere in that alert The Article 29 Working Party approach is not being adopted uniformly and data protection authorities are responding to complaints and issuing requests for information. Its important to develop a plan so that you know what you need to do but also so that you can show a**

complaint or regulator that you are aware of the need to take action.

2. Take stock. Map out your data flows. What information travels outside of Europe? On what basis? Is it inter-group or is it to third parties? Are they using Safe Harbor as an exemption, or do you already have other comfort?
3. Check your contracts with your third party suppliers who use safe harbor. Do they deal with this situation? It might be time to start a dialogue.
4. Equally, if you are a supplier who relies on safe harbor to legitimise your processing activities, make sure this ruling doesn't put you in breach of any of your contracts, and perhaps consider reaching out to your affected customers.

And then:

1. Take a look around. Once the dust has settled, options may seem clearer.
2. Consider the options available to your business. In summary, at the present time they are:
    1. Stop transferring personal data to the US – site your servers in Europe, for example. This may be a draconian suggestion for some businesses, but for others might be a relatively easy switch.
    2. Put in place Model Form Data Transfer Agreements. In many ways, these are a really easy fix. The European Commission has already drafted them for you, and you shouldn't change any of their terms. But they are legally binding documents which impose obligations on both parties which should be clearly understood – you shouldn't enter into them lightly. They also need to be entered into between data controller and data processor, and so for suppliers, this can be a time-consuming and paper-heavy process.
    3. Consider moving to Binding Corporate Rules. We've recently discussed this process, and their inclusion in the new Data Protection Regulation are a sign post to their importance going forward. This shouldn't be a knee-jerk reaction as Binding Corporate Rules require a corporate "buy-in" to the protection of personal data; but this is indeed their strength, and businesses who took adherence to Safe Harbor seriously may find that they are a long way down the path to making the changes required for Binding Corporate Rules. They are not an overnight solution, however, as even once you have your house in order, the negotiation process with the data protection authorities can take some months; but you may want to consider getting in quick before they are submersed in requests! **[03.11.15] BCRs are also not a catch-all solution. Some data protection authorities currently have no BCR option for data transfer. On 23 October the Portuguese Data Protection Authority (Comissão Nacional de Protecção de Dados or CNPD) issued its response to the Schrems decision and reminded companies that BCRs are not an option yet in Portugal. The CNPD statement (in Portuguese) is** here.
3. Remember that the EU and the US are already in negotiation over replacing Safe Harbor and no doubt a new urgent impetus has been injected into this process.

How does this affect the US-Swiss Safe Harbor Framework

Technically at the moment, it doesn't at all, as the Swiss legal regime is not bound by the European Court of Justice.

However, the Federal Data Protection and Information Commissioner (FDPIC), the regulator in Switzerland, issued a press release on 6 October stating that the agreement between Switzerland and the USA is also called into question by this decision. It has recommended that Swiss organisations who transfer data to the US should enter into contractual terms with their providers. Indeed, it has also recommended that data should be stored by European providers on servers in Europe. **[03.11.15] On 7 October FDPIC repeated this advice in a short guidance note which is** here.

Response from Regulators

National regulators like the UK's Information Commission Office have already been issuing press releases in response to today's judgment. The ICO's press release states that it will take businesses "some time" "to review how they ensure that data is transferred to the US in line with the law" and that they will be working with other data

regulators to issue guidance to help businesses. The ICO takes care to point out that this judgment does not indicate that there is any increase in threat to personal data; but that businesses must take steps to protect it.

Across Europe, many regulators are embracing the decision as a significant day for Data Protection. A key element of this seems to be driven by the fact the decision could help reduce complacency, and encourage data controllers to consider data transfers on their own merits, rather than simply signing up to a global scheme and forgetting about them. This very much echoes the focus on privacy impact assessments in the new Regulation.

[20.10.15] The regulators in their combined force as a Article 29 Working Party have issued a useful and pragmatic statement. Although they are seeking a much better solution by the beginning of next year, they have confirmed that transfers under Model Contracts or Binding Corporate Rules are currently unaffected by the decision. For more information on this statement, please see our report here.

However, one of the German data protection authorities, based in Schleswig-Holstein, has taken a rather contrary view. If you are transferring data from this region, the authority has stated that there are very few justifications for a transfer to the US at the present time, and none that apply to employees. They have also noted their ability to fine up to €300,000 for any breach. For more information, please see our report here.

[03.11.15] The Schleswig-Holstein lead has been largely adopted by other German data protection authorities who issued a joint statement on 26 October. For more information on that statement see our report here.

[03.11.15] The response from other data protection regulators has been more measured. For example Finland's Data Protection Ombudsman (Tietosuoja) issued a statement on 22 October saying that companies and individuals using online services which previously had the benefit of Safe Harbor *"will now have to re-evaluate their use of these services".* The Ombudsman issued five instructions which largely follow the Article 29 Working Party Statement.

[10.11.15] The Italian data protection authority (Garante Per La Protezione Dei Dati Personali) issued a substantially similar statement on 6 November 2015. Our summary of that statement is here.

The European Commission in its press conference on 6 October made sure to state that it remains fully committed to data transfers across the Atlantic, and echoed our suggestions above as to how data flows can be maintained in the meantime.

[19.11.15] In an official Communication of 6 November the European Commission has also come out in support of Model Clauses and Binding Corporate Rules. Our summary of that statement can be found here.

Nonetheless, it was at pains to point out that it had made 13 recommendations on how to make safe harbor safer following the Snowden revelations.

They have already started the process of working with the Article 29 Working party and will work with local data protection authorities to avoid fragmentation and develop a co-ordinated approach.

Effect on Regulators

As far as the new Regulation is concerned, the European Commission noted that the ruling underlines the additional powers of data protection authorities under consideration in the current draft, making clear that they saw no interference in the expected timeline for the Regulation by this judgment.

However, more generally as regards enforcement, as a result of the judgment there is nothing now to stop national data protection regulators undertaking investigations and suspending data transfers where the latter action is appropriate.

This begs the question as to whether other possible complaints might be brought before national data protection

regulators against US internet businesses such as Google, Yahoo, Microsoft, and Apple in the same context. Whether the regulators are ready for this is one issue but equally some businesses may need to consider this as a possibility.

Although the legislation seems to be moving towards a principle of "one stop shop" for data protection compliance, this case, together with this month's other headline case of Weltimmo, seems to be taking a different approach.

US Response

[21.10.15] On the US side there are also some moves towards a more lasting solution. The US House of Representatives agreed on 20th October to move forward the Judicial Redress Bill, which would seek to allow some foreigners the right to pursue their privacy rights in US courts – one of the European Court's objections in the Schrems case. Congressman Jim Sensenbrenner who introduced the Bill said:

> **"The sudden termination of the Safe Harbor framework strikes a blow to U.S. businesses by complicating commercial data flows. If we fail to pass the Judicial Redress Act, we risk similar disruption to the sharing of law enforcement information. If we fail to pass the Judicial Redress Act, we will undermine several important international agreements, further harm our businesses operating in Europe, and severely limit sharing of law enforcement information…The Judicial Redress Act currently enjoys broad support and has been endorsed by the Department of Justice as well as the U.S. Chamber of Commerce and numerous U.S. businesses… Let's put the President's infamous pen to good use signing this legislation."**

You can see the full speech here **and monitor the Bill's progress** here**.**

Background

In brief: Following the Snowden US surveillance revelations in 2013, Austrian citizen Maximillian Schrems brought a legal challenge before an Irish court challenging his rejected complaint before the Irish data protection regulator claiming that the US does not offer protection against surveillance by US intelligence authorities of data transferred to the US from the EU - Schrems' data was being transferred from Facebook's Irish subsidiary to the US. Back in 2000 the EU adopted the Safe Harbor Decision which provides a legal scheme for the adequate protection of personal data from the EU to the US whereby US businesses could self-certify. As the issue involved an interpretation of EU data protection law the Irish court had to refer to the European Court the question of whether the 2000 Safe Harbor Decision stops a national data protection regulator from investigating a complaint claiming that a country doesn't ensure an adequate level of data protection and where appropriate from also suspending the contested personal data transfer. The European Court has today ruled that not only does a national court have such powers but that in addition the Safe Harbor Decision is invalid.

Jonathan Armstrong, Gayle McFarlane and André Bywater are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

Gayle McFarlane, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 118 2700

André Bywater, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com