Client Alert: Swiss Privacy Shield Collapses

Date : September 8, 2020

Introduction

In July we wrote about the latest instalment of the battle between privacy activist Max Schrems, Facebook and Ireland's Data Protection Commission. We looked at the European Court of Justice ('the European Court') striking down the EU-US Privacy Shield data transfer scheme. Today the Swiss authorities effectively followed the European Court's decision and struck down the Swiss-US Privacy Shield too.

You can read more about the European Court's decision here https://bit.ly/pshielddead and see our short film on the issues here https://bit.ly/Schrems3film.

Today's ruling does not just affect the 5,256 businesses registered in the Swiss Privacy Shield scheme. Given the additional focus on due diligence in any data transfer, every organisation will have work to do to make sure it complies with both EU and Swiss data transfer rules.

Background

Switzerland formerly had a Safe Harbor scheme in place similar to the EU-US Safe Harbor scheme struck down by the European Court in the original Schrems decision in 2015. Like the EU-US scheme a new Privacy Shield scheme was agreed between Switzerland and the US to replace Safe Harbor. That scheme was announced in January 2017 and introduced in April 2017.

Following the European Court decision, the Swiss Federal Data Protection and Information Commissioner (FDPIC) said that he was reviewing the Swiss Privacy Shield. He said on 16 July 2020 "*The FDPIC has taken note of the CJEU ruling. This ruling is not directly applicable to Switzerland. The FDPIC will examine the judgement in detail and comment on it in due course.*"

Today the FDPIC published his annual report into the Swiss-US Privacy Shield scheme. He said that he had taken into account the European Court's decision on EU-US Privacy Shield and he had reassessed the scheme's compliance with Swiss law.

The FDPIC said that after an in-depth analysis, he had come to the conclusion that even if it guaranteed some rights to people in Switzerland, Privacy Shield did not offer an adequate level of protection as required by Swiss data protection law. He stressed however that the Swiss decision has no bearing on the continuation of the Privacy Shield regime and data subjects can invoke it until it is revoked by the US authorities. For many businesses this is the worst of all worlds – a removal of the protection which Privacy Shield brings them for data transfers but the continuance of the burden of complying with the scheme's requirements with the possibility of sanction in the US if they fail to comply.

Takeaways

In our view every business should work on a data transfer response plan. Even if this is a work in progress it might be something that they can show a regulator or a complainant if they come knocking. We can expect more questions about data transfer as a result of today's ruling, especially from Swiss-based employees. Putting a data transfer plan together is a strategy which we used after the fall of Safe Harbor and it worked well for many then. The plan might also be something that will reassure customers and other stakeholders. That plan might include:

1. Thinking about how you transfer data. If you rely on Privacy Shield you will need to look at another way. You may also wish to consider your continued involvement in the Privacy Shield scheme given that it may still provide burdens but with little benefit;
2. It is also important to look at how those you do business with those who have used Privacy Shield to legitimise data transfers too – for example if you have a global HR platform, a global payroll provider, a

travel management company or a whistleblowing helpline, they may rely on Privacy Shield. You can check to see if they are on the list here - https://www.privacyshield.gov/list If they are you'll need a new plan and it is important to contact those you do business with now – we saw after Safe Harbor was struck down that queues for assistance developed very quickly. In some sensitive areas you might want to look at securing service providers in Europe instead;

3. In a post-GDPR world employees and customers are likely to ask questions about the way in which you make data transfers lawful. Be ready for their questions. Some prepared FAQs may help HR teams and contact centres respond to these questions. Works councils are also likely to ask questions too; and
4. Look at your transparency obligations. Many organisations specifically refer to Privacy Shield in their privacy policies for example – these will therefore need updating. You might need to alter other documents too including internal notices to employees;

You can read today's announcement in French here https://bit.ly/35n4kCC

For other articles that we have written about data protection issues please see here: https://www.corderycompliance.com/news/

For details about Cordery's GDPR Navigator subscription service, which includes short films, straightforward guidance, checklists and regular conference calls to help you comply, please see here: www.bit.ly/gdprnav.

For more information please contact Jonathan Armstrong or André Bywater who 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

André Bywater, Cordery, Lexis House, 30 Farringd
Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com