Privacy Shield FAQs

Date : October 19, 2018

These FAQs answer some basic questions on Privacy Shield. We use some technical terms which are explained in our glossary here - http://www.corderycompliance.com/eu-data-protection-regulation-glossary/. If you would like detailed advice on Privacy Shield we are happy to help – our contact details are at the end of these FAQs.

What is Privacy Shield?

The Privacy Shield scheme was proposed in February 2016 to replace the Safe Harbor scheme which was struck down by the European Court of Justice (ECJ) in the first Schrems case (sometimes known as Schrems 1) in October 2015. There is some background to the collapse of Safe Harbor and the announcement of Privacy Shield in our alert on 3 February 2016 here - http://www.corderycompliance.com/safe-harbor-safe/.

Why did it take so long?

As we said in February 2016 the announcement of the creation of Privacy Shield was premature. An announcement had to be made in February 2016 as a deadline set by the Article 29 Working Party (often known as WP29) had expired at the end of January 2016. In February 2016 the European Commission said that they hoped that Privacy Shield would be finalised by the beginning of May 2016. Even that seemed ambitious in part because of the criticism that Privacy Shield received from WP29 in April 2016. You can see a summary of WP29's criticisms of Privacy Shield in our alert and short film here - http://www.corderycompliance.com/wp29-refuse-to-endorseprivacy-shield-scheme/.

When did Privacy Shield come in?

The scheme opened for business on 1 August 2016.

Who has joined so far?

More than 3,820 organisations have joined Privacy Shield. They include Ernst & Young, Facebook (for non HR data only), Google, Microsoft, Oracle, Rackspace, Salesforce, ServiceNow, St Jude Medical and Workday. Some organisations have already let their Privacy Shield certification lapse. On 16 October 2018, according to the US Department of Commerce, 361 organisations who had self-certified to Privacy Shield were no longer active participants.

If I join Privacy Shield will the US authorities play a greater role?

Almost certainly.

There is likely to be more supervision by the US authorities than there was under Safe Harbor. It is not true to say there was no Safe Harbor enforcement (for example we looked at the investigation into TRUSTe here - http://www.corderycompliance.com/further-safe-harbor-enforcement-from-the-federal-trade-commission/) but both the European Commission and the European Parliament have called for tougher enforcement.

Is Privacy Shield bullet proof?

Probably not.

Penny Pritzker, the former US State Secretary of Commerce, said on 12 July 2016 in announcing the deal that she thought it would 'withstand scrutiny' and that she had been speaking with the chair of WP29 to try and reduce her concerns. Commissioner Jourová also said she was confident it would survive a court challenge. In our view it is unlikely that the concerns about Privacy Shield will disappear so quickly. We talked about the challenges to Privacy

Shield when we spoke with Max Schrems on 21 October 2016. You can find a summary of that interview here - http://www.corderycompliance.com/interview-with-max-schrems/. Max Schrems said in that interview "Privacy Shield is Safe Harbor with flowers on it – it will probably be killed by the European Court".

The successful challenge to the EU – Canada PNR data sharing agreement in July 2017 would suggest that the ECJ's position has not changed too much since the original Schrems decision.

As well as possible challenges from courts and regulators it should be remembered that Privacy Shield is reviewed annually. The European Commission, perhaps not unsurprisingly, gave a qualified pass on its first review. WP29 was more critical announcing the results of their first review on 1 December 2017. WP29 said that it had identified *"a number of significant concerns"* and called upon the European Commission and the relevant authorities in the US to restart discussions. Commissioner Jourová met with WP29's successor, the European Data Protection Board on 26 September 2018 to hear its concerns. The European Parliament in particular has been looking carefully at the scheme. In July 2017 Claude Moraes the Chair of the European Parliament Committee looking at the Privacy Shield annual review said: *"Deficiencies still remain and must be urgently resolved to ensure that the Privacy Shield does not suffer from critical weaknesses"*. On 12 June 2018 the European Parliament's Civil Liberties Committee (also called the LIBE Committee) said that Privacy Shield should be suspended on 1 September 2018 if improvements have not been made by then.

We understand that Commissioner Jourová wrote to the US administration on the 26 July 2018 saying that the US administration needed to take action to save Privacy Shield by the 26 October 2018. We understand that as a result, US Secretary of Commerce Wilbur Ross has agreed to meet with Commissioner Jourová in Brussels in October 2018 as part of the Privacy Shield annual review process. In an effort to meet some of Europe's concerns the US appointed a new Privacy Shield Ombudsperson, Manisha Singh, in September 2018. The US Federal Trade Commission (FTC) also took action in September 2018 against four companies who falsely claimed that they were part of the Privacy Shield scheme.

Could it be challenged by Regulators?

Almost certainly.

Reports in August 2016 suggest that Johannes Caspar, the Hamburg Data Protection Regulator who had been very critical of Safe Harbor, would like to refer the scheme to the ECJ. Caspar has petitioned the German authorities to allow data protection regulators to refer issues like this to the ECJ directly.

In November 2016 ten German data protection authorities announced that they had sent a survey to 500 organisations asking for details of their data protection strategy. Around 150 of these questionnaires were sent by the Bavarian Data Protection Commissioner. Initially the businesses had been sent a questionnaire for them to complete and return to the relevant regulator. The document asks specific questions about the business' use of Privacy Shield and other methods of dealing with international data transfer. Additionally the questionnaire asks for details of specific data transfers to the USA including in areas like helpdesk support, travel management, CRM, marketing, recruitment, collaboration platforms, quality management and cloud.

Privacy Shield is certainly open to challenge in the same way as Safe Harbor was.

What about a court challenge?

Privacy Shield faces several court challenges and the Schrems 1 case tells us that DPAs must have more independence to investigate their concerns. A second case from Ireland involving Mr Schrems has also now been referred to the ECJ and questions have been asked in that referral about Privacy Shield.

Whilst a challenge does seem likely there is no guarantee that would succeed. A differently constituted court on a different day may be more willing to uphold Privacy Shield especially with the extra effort that both the EU and US have made this time around. Whatever the result however there is likely to be uncertainty since a court hearing may be unlikely before the end of 2018 on current court timetables.

Is Privacy Shield protected by GDPR?

No.

Privacy Shield is not referred to in GDPR although one of the other methods of data transfer, Binding Corporate Rules (or BCRs) is.

Should I even consider Privacy Shield for my business?

Possibly.

Despite its faults those companies who were in Safe Harbor might find Privacy Shield fairly easy to achieve. It could have some role as part of a mix of compliance measures, although it is unlikely to provide a complete solution on its own. It would be wise for those considering the scheme to do a cost-benefit analysis. Privacy Shield is likely to be more costly than Safe Harbor – in part due to higher arbitration costs – but may demonstrate a level of compliance to some of your customers. Some of the former Safe Harbor arbitration schemes have also adapted themselves to manage Privacy Shield arbitrations.

Are there any deadlines?

No but there were concessions for businesses that signed up to Privacy Shield before the end of September 2016. That concessionary period, which applied to existing onward transfers of data, has now ended.

How much will it cost to join Privacy Shield?

As well as the arbitration scheme cost an organisation must pay an annual fee to the US Department of Commerce (DoC). That fee is tiered based on the organization's annual revenue and ranges from $250 to $3,250. Additionally there is a fall-back arbitration scheme which will be funded by a levy on Privacy Shield participants.

If I join will I have to change my website privacy policy?

Probably.

Privacy Shield has some quite detailed requirements on what a privacy policy should say. The first Privacy Shield Principle deals with the notice that has to be given but there are additional requirements in connection with information about arbitrations and other rights that individuals have with respect to their personal data. If you are joining Privacy Shield you will need to review your privacy policy to make sure it complies before you apply.

What about Swiss transfers?

A similar Privacy Shield scheme for transfers from Switzerland has been operational from April 2017. Details are here: http://www.corderycompliance.com/client-alert-new-privacy-shield-scheme-in-switzerland/.

What can I do?

In short to get started, the following are possible actions to take:

- Have a plan for data transfer – we have seen from some of the enforcement cases that the lack of a plan is likely to cause difficulties when regulators ask questions.
- Review Privacy Shield to see if it might work for you – even a system subject to a challenge may be useful or you.
- Look again at your data flows to determine the following: what information travels outside of the EU and on what basis? Is it inter-group or is it to third parties? What steps are already in place to make those data flows lawful? You may be able to alter your current data practices to reduce your risk.
- Consider the other options available to your business including model clauses (recognizing they are also

subject to challenge) and BCRs. BCRs do have a new footing in GDPR and may be more resistant to challenge. BCRs will not be the answer for everyone however.

- Review your privacy policy. Some organisations have not reviewed their policy since the fall of Safe Harbor in October 2015. Whichever way you make your data transfers lawful you should still be reflecting your current practices in your privacy policy.

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

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

André Bywater

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com