Using the privacy shield to transfer data to the US

Data Protection Act

Contents

Background 2
The Privacy Shield 2
What should I do? 3
What options are there? 4
What if I am using a cloud-based service? 4
What does the Schrems judgment say? 5
Does the Schrems judgment affect the other transfer mechanisms? 5
How does the judgment affect the powers of data protection authorities? 5
What is the ICO doing? 6
How can I get more information? 6

Background

1. Under the eighth data protection principle organisations that want to transfer personal data outside the EU must assess whether that country ensures an adequate level of protection for individuals. The European Commission can decide whether countries are considered adequate, either partially or fully.

2. On 6 October 2015 the Court of Justice of the European Union (CJEU) issued its judgment in Schrems v Data Protection Commissioner (Ireland) ("Schrems"). This judgment removed the assurance that using Safe Harbor had previously given to businesses, ruling that it did not provide adequate protection.

The Privacy Shield

3. The EU-US Privacy Shield replaces the Safe Harbor framework. It is a binding legal instrument under European law which can be used as a legal basis for transferring personal data to the US.

4. On 12 July 2016 the European Commission issued its formal adequacy decision on the Privacy Shield, after consulting and considering recommendations from the Article 29 group of EU data protection authorities (which includes the ICO).

5. The Shield contains many stronger privacy requirements than under Safe Harbor. There are stronger obligations on the companies who receive data to provide greater transparency about the processing they are undertaking and tighter restrictions for onward transfers. The US Department of Commerce has greater oversight mechanisms with options to apply sanctions and exclusions to companies who do not comply with the rules.

6. The Privacy Shield documents contain assurances from the US government that any access by their public authorities to personal data transferred under the Shield will be subject to clear limitations, safeguards and oversight mechanisms.

7. Data subjects also have several redress possibilities, either with the companies themselves, their Data Protection Authority or with an independent arbitration mechanism.

8. There will also be a unique annual joint review mechanism, where European Data Protection Authorities will join the

European Commission to assess whether the Shield is functioning effectively and providing sufficient safeguards. The first annual joint review will take place in September 2017. The ICO remains actively involved in the work to review the workings of the Privacy Shield.

9. The scheme became operational on 1 August 2016 when the US Department of Commerce started to receive certifications from US organisations. You can check the list of companies who are certified to receive data under the Privacy Shield on https://www.privacyshield.gov/list.

10. The European Commission's guide for citizens further explains a Privacy Shield company's obligations and what individuals can expect from a company that has signed up to the scheme.

What should I do?

11. You should have already reviewed your position if you were relying on Safe Harbor as a legal basis for transfers of personal data to the US. The law, both under the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR), says you can only transfer personal data with adequate protection, and Safe Harbor does not give that protection. Doing nothing is not an option.

12. Any transfers that continue solely under the Safe Harbor framework will breach the eighth data protection principle. In these circumstances we could contemplate enforcement action, in line with ICO enforcement policies. Organisations should already have made the relevant changes, but if not, the key is not to delay.

13. You should consider:

- what personal data you are transferring outside the EU;
- where it is going to;
- what arrangements you have made to ensure that it I adequately protected; and
- whether these arrangements are the most appropriate ones, taking into account the ICO's guidance on assessing adequacy.

What options are there?

14. The Privacy Shield is one of a number of mechanisms for transfers of personal data to the US. A good first step is to see whether the US organisations you transfer personal data to are looking to become part of the Privacy Shield scheme. The Department of Commerce in the US will oversee certification under the scheme, and has launched a dedicated website that offers advice to businesses. If the company you want to transfer data to is not certified, you cannot rely on the Privacy Shield.

15. Alternatively you can use Standard contractual clauses (SCCs) and binding corporate rules (BCRs). These are not the only options and you can find more information in ICO guidance on the eighth principle.

16. Businesses in the UK do not have to rely on Commission decisions on adequacy. Although you won't get the same degree of legal certainty, UK law allows you to rely on your own adequacy assessment. Our guidance on assessing adequacy tells you how to go about doing this. Much depends on the nature of the data you are transferring and who you are transferring it to. However the main question is whether you can reduce the risks to the personal data, or more importantly the individuals whose data it is, to a level where the data is adequately protected after transfer.

What if I am using a cloud-based service?

17. The use of cloud computing has increased in the global market providing an efficient tool for individuals and business (including small and medium size enterprises). The main concern about cloud computing is the location of the data centres and servers used by the cloud service providers to store data.

18. We expect that many cloud service providers wishing to provide services in Europe will be carrying out reviews of their contractual arrangements and the mechanisms underpinning any transfers of personal data from Europe.

19. As a business or individual, it would be advisable to look at your cloud service provision and find out whether your personal data is being held overseas or on servers based in the European Economic Area.

20. The ICO guidance on cloud computing remains a useful source of information and assistance in this area.

What does the Schrems judgment say?

21. There are two reasons why the CJEU struck down the Commission Decision. Firstly because the US intelligence services had the ability to gain access to transferred personal data to an extent that goes beyond what is strictly necessary and proportionate for the protection of national security. Coupled to this was a lack of any right for non-US persons to seek legal remedies in the USA for misuse of their data.

22. The second element was the CJEU's ruling that data protection authorities can examine claims from individuals that their data has not been properly protected, even where there is a Commission Decision on adequacy.

Does the Schrems judgment affect the other transfer mechanisms?

23. The CJEU only invalidated the Safe Harbor Decision. The existing Commission Decisions on the adequacy of particular countries and on Standard Contractual Clauses still stand and businesses can rely on these, certainly for the time being. Binding Corporate Rules can still be used.

How does the judgment affect the powers of data protection authorities?

24. One effect is to reaffirm that data protection authorities have the power to investigate any complaints about the transfer of personal data even if the Commission has made a finding of adequacy,

25. The ICO position remains the same; whilst complaints can be considered, the usual ICO regulatory policy will be applied. We will be guided by the risk posed to individuals and steps that can be reasonably expected of data controllers. The Article 29 group of EU data protection authorities (of which the ICO is an active member) have given their collective view on the new agreement. Their latest statement reflects on the final version of the Shield and the changes that were made in response to

the opinion it issued in April 2016. The annual review process will help assess how well the system is working.

26. The area of international transfers is still uncertain. The CJEU is currently considering cases that may impact on other mechanisms for international transfers. The Court may also be asked to consider whether Standard Contractual Clauses provide adequate protection for transfers to the US.

What is the ICO doing?

27. The ICO will consider complaints from affected individuals whatever transfer mechanism you're relying on but we will be keeping to our published enforcement criteria and not taking rushed action whilst there's so much uncertainty and solutions are still possible.

28. The ICO aims to provide guidance to organisations to help them remain compliant. We recognise that most organisations want to do all they can to comply.

29. We will continue to work with our European counterparts in an effort to ensure that, as far as possible, we are delivering a single and sensible message.

How can I get more information?

30. We have updated our guidance on international transfers to cover the Privacy Shield. We intend to build on this guidance by publishing some practical advice for businesses, including SMEs that may rely on cloud and similar services provided by others, on what they should and should not be doing. This advice will be developed in conjunction with our guidance on international transfers under the GDPR. We'll also update the information we provide to the public through our website.

31. In the meantime, you may find the following sources of information useful:

    - The Article 29 Working Party statement on the consequences of the Schrems judgment (published 3 February 2016).
    - The European Commission communication on the international transfer of personal data (published 6

November 2015; based on guidance from the Article 29 Working Party).

- Article 29 opinion on the decision of the European Commission on the EU-US Privacy Shield (published 26 July 2016).
- European Commission guide for citizens.
- The US Department of Commerce dedicated website https://www.privacyshield.gov.