Data transfers to the US and Safe Harbor – interim guidance

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 invalidated the Decision of the European Commission in 2000 which had found that US Safe Harbor provided adequate protection for personal data transferred from the EU to Safe Harbor member companies in the USA.

What is Safe Harbor?

The US-EU Safe Harbor framework is a self-regulatory system, with some statutory underpinning, in which member companies in the USA sign up to Privacy Principles and a complaints system. Oversight of the system is provided by the Federal Trade Commission amongst others. The effect of the Commission Decision was to give businesses an assurance that if they transferred personal data to Safe Harbor members in the USA they would satisfy the legal requirement for personal data transferred outside the EU to be adequately protected.

What does the Schrems judgment say?

There are two elements to the judgment. First the reason why the Court struck down the Commission Decision was because of the ability of the US intelligence services to gain access to personal data transferred to an extent that goes beyond what is strictly necessary and proportionate for the protection of national security. Coupled to this is a lack of any right for non-US persons to seek legal remedies in the USA for misuse of their data. The second element was that the CJEU ruled that, even where there is a Commission Decision on adequacy, data protection authorities are not prevented from examining claims from individuals that their data have not been properly protected.

Does the Schrems judgment affect the other transfer mechanisms?

It is important to remember that it was only the Safe Harbor Decision that the CJEU invalidated. The existing Commission Decisions on the adequacy of particular countries and on standard contractual clauses still stand and can be relied on by businesses, certainly for the time being and Binding Corporate Rules can still be used.

Even so, the terms of the judgment inevitably cast some doubt on the future of the Decisions relating to these other mechanisms given that data transferred under them are also liable to be accessed by intelligence services, whether in the USA or elsewhere. The impact on these other mechanisms and on transfers to destinations other than the USA is far from clear and is being analysed by the Article 29 Working Party of European data protection authorities amongst others.

What is happening to Safe Harbor now?

On 2 February the European Commission announced a new framework to replace Safe Harbor: the EU-US Privacy Shield. The Shield is yet to be assessed by the Article 29 Working Party and is not yet a formal adequacy decision of the European Commission. In the meantime Safe Harbor can still be seen as providing a measure of protection for data transferred from the EU to the USA but businesses should be aware that the certainty of an adequacy decision of the Commission has now been removed and they should make their own assessment of risk to compliance.

What are the data protection authorities doing?

One effect of the Schrems judgment is the recognition of the extent of the powers of the data protection authorities, which is not confined to the Safe Harbor Decision. Other Commission findings on the adequacy of particular countries and on standard contractual clauses can no longer override the rights of individuals to have complaints about the protection of their personal data considered by data protection authorities, including the ICO. Although the ICO approach to considering complaints will not suddenly change it is inevitable that some of the legal certainty that Commission findings of adequacy have provided for businesses in the past will no longer be available.

The data protection authorities have been meeting and considering the implications of the Schrems judgment including comparative analysis of the legal position in the EU and in the USA.

The European Commission has also produced a communication on the international transfer of personal data which is based on guidance from the Article 29 Working Party of European data protection authorities.

The data protection authorities recognise the importance of working together but it is clear that solutions do not lie in our hands alone.

The Article 29 Working Party will now start the process of assessing the proposed EU-US Privacy Shield.

Article 29 published a statement on consequences of the Schrems judgment on 3 February.

What is the ICO doing?

We are not rushing to use our enforcement powers. There is no new and immediate threat to individuals' personal data that has suddenly arisen that we need to act quickly to prevent. Of course the ICO will consider complaints from affected individuals whatever transfer mechanism you're relying on but we will be sticking to our published enforcement criteria and not taking rushed action whilst there's so much uncertainty around and solutions are still possible. We can't create legal certainty where there is none but we will continue to work with our European counterparts in an effort to ensure that, as far as possible, we're all delivering a single and sensible message. Ultimately though, for the ICO, it has to be a message that is consistent with UK law, with our powers and with the public commitments we have made about when and how we will use these powers.

In time we will update our published guidance on international transfers but for the most part it is still valid. We will also be building on this interim 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 in the current period of uncertainty.

What should I do?

As we have been saying from the outset - don't panic and don't rush to other transfer mechanisms that may turn out to be less than ideal. The impact of the judgment on standard contractual clauses and binding corporate rules is still being analysed. Of course transfers can always be made on the basis of an individual's consent but this does not necessarily protect personal data any more effectively than the Safe Harbor which is, after all, what the CJEU case is all about. Indeed, individuals may be easily induced to give their consent to the transfer of their data to destinations where there is little or no protection when the Safe Harbor does at least provide them with some genuine protection even if such protection is imperfect.

The first thing for businesses to do is take stock. Ask yourself what personal data are you transferring outside the EU, where is it going to,

and what arrangements have you made to ensure that it is adequately protected. For some this will be no easy task. Then look at whether these arrangements are the most appropriate ones, taking into account the ICO's guidance on international transfers.

But don't rush to change whilst the process to assess the Shield is ongoing.

It is also worth bearing in mind that businesses in the UK don't 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 tells you how to go about doing this. Much depends here on the nature of the data that you are transferring and who you are transferring it to but the big question is can you reduce the risks to the personal data, or rather the individuals whose personal data it is, to a level where the data are adequately protected after transfer?

What if I am using a Cloud-based service?

In recent years, cloud computing has played an increasingly strong role 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.

As we said before, there is no need to rush to change anything you are currently doing, but 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 in order to guarantee EU data protection standards for data in the cloud.

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 EEA.

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