

SAFE HARBOR NO MORE BUT ARE THERE CALMER WATERS AHEAD?

by Claire Milne WS

April 2016

As we reported in our October 2015 edition of the Isle of Man Regulatory Update, the Court of Justice of the European Union (**CJEU**) ruled on 6 October 2015 (the Schrems case - Case C-362/14) that organisations cannot rely on the European Commission approved Safe Harbor scheme when transferring personal data from the European Union (**EU**) to the United States of America (**US**).

Background

The EU's Data Protection Directive 95/46/EC (**Directive**) provides that personal data may only be transferred to a country outside the European Economic Area (**EEA**) if that country ensures an adequate level of protection for the data. This corresponds to the "Eighth Data Protection Principle" as it is set out in the Isle of Man's Data Protection Act 2002. The European Commission has certified that a number of non-EEA countries do provide "adequate protection" and the Isle of Man is one of these jurisdictions (so called "adequacy decisions"). In relation to the US, the Commission developed so called "Safe Harbor" arrangements whereby US companies could be certified as providing adequate protection. It was a self-certification scheme operated by the US Federal Trade Commission and provided a US company had a Safe Harbor certification, the transfer of personal data to it was permitted and complied with the terms of the Directive.

Safe Harbor arrangements had come under increased scrutiny and criticism following Edward Snowden's revelations in 2013 about US security agencies accessing personal data, all of which culminated in the CJEU's decision in the Schrems case.

The Safe Harbor provisions underpinned a number of commercial arrangements and transfers between the US and the EU and it has been a difficult few months for many organisations to put in place replacement

provisions. The other mechanisms to allow compliance with the Directive, such as use of EU Model Contracts and Binding Corporate Rules, still apply post the CJEU's decision in the Schrems case. However, since the decision, the European Commission has been trying to develop a replacement to the Safe Harbour provisions and it announced the new arrangement for transatlantic data flows on 2 February 2016 - the EU-US Privacy Shield.

The EU-US Privacy Shield

The new proposed arrangements include the following elements:

- US companies wishing to import personal data from the EU will need to commit to robust obligations on how personal data is processed and individual rights are guaranteed. The US Department of Commerce will monitor that companies comply with their commitments, which are legally enforceable under US law by the US Federal Trade Commission.
- Any company handling human resources data from the EU has to commit to comply with decisions by EU data protection authorities.
- For the first time, the US has given the EU written assurances that access by public authorities of personal data for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. These exceptions must be used only to the extent necessary and must be proportionate. The US has ruled out indiscriminate mass surveillance on the personal data transferred to the US under the new arrangement. To regularly monitor the functioning of the arrangement there will be an annual joint review, which will also include the issue of national security access. The European Commission and the US Department of Commerce will conduct the review and invite national intelligence experts from the US and EU data protection authorities to it.
- Any EU citizen who considers that his data has been misused under the new arrangement will have several redress possibilities. Companies will have 45 days to reply to complaints. EU citizens can take complaints to their "home" data protection authority that can then refer complaints to the US Department of Commerce and the US Federal Trade Commission. In addition, Alternative Dispute resolution will be free of charge. For complaints on possible access by national intelligence authorities, a new Ombudsperson will be created.
- US companies will require to register to be on the Privacy Shield List and self-certify that they meet the requirements. This procedure has to be done each year. The US Department of Commerce will have to monitor and actively verify that companies' privacy policies are presented in line with the relevant Privacy Shield Principles and are readily available. The US has committed to maintaining an updated list of current Privacy Shield members and removing those companies that have left the arrangement. The Department of Commerce will ensure that companies that are no longer members of Privacy Shield must still continue to apply its principles to personal data received when they were in the Privacy Shield, for as long as they continue to retain such data.

On 29 February 2016, the European Commission issued the legal texts that will put in place the EU-US Privacy Shield and also made public a draft adequacy decision. This included the "Privacy Shield Principles" US companies have to abide by, as well as written commitments by the US Government (to be published in the US

Federal Register) on the enforcement of the arrangement, including assurance on the safeguards and limitations concerning access to data by public authorities.¹

Once adopted, the Commission's adequacy finding establishes that the safeguards provided when data are transferred under the new EU-US Privacy Shield are equivalent to data protection standards in the EU.

Why Does this Matter in the Isle of Man?

The Isle of Man's Data Protection Act 2002 (**DPA**) is based on the Directive. The terms of the Eighth Data Protection Principle under the DPA states that "personal data shall not be transferred to a country or territory outside the Island unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data." Under paragraph 23 of Schedule 1 of the DPA, if transfers are made to countries within the EEA, they are presumed to have an adequate level of protection. In addition, if the European Commission has made an adequacy finding in relation to the transfer in question then such will have effect under the DPA. This issue therefore does impact on Isle of Man entities wishing to transfer personal data to the US.

What Now?

In accordance with Article 30(1)(c) of Directive 95/46/EC, the Article 29 Working Party (which is composed of representatives of the national data protection authorities, the European Data Protection Supervisor and a representative of the European Commission) will assess the relevant documents in order to give its opinion on the level of protection afforded by the EU-US Privacy Shield. At the time of writing, the Article 29 Working Party's opinion is expected in April or May. Following the Working Party's opinion, the next steps in the procedure before the adoption of the adequacy decision by the European Commission will be the opinion of the Member States in comitology, in accordance with Article 31 of the Directive. Therefore, there are still hurdles to be jumped before the process is complete and even if the proposed adequacy decision is adopted then its validity can still be questioned by the CJEU, as we saw in the Schrems case last year.

The Isle of Man Information Commissioner (previously called the Data Protection Supervisor) issued a note in December 2015 stating that following the Schrems case (and communications issued by the European Commission after the case) and in light of the proposed new EU General Data Protection Regulation, it is likely that the Island's adequacy decision, in its entirety, will be subject to review by the European Commission. It seems that those calmer waters may be a while off yet.....!

This article has been written by:

Isle of Man

Claire Milne WS

Partner

cmilne@applebyglobal.com

Claire Milne is Partner in the Corporate Department at Appleby. A copy of this article is available on the firm's web site at applebyglobal.com

¹ See http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf for a copy of the draft adequacy decision and see http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf for details of the Privacy Shield Principles.

This publication is for general guidance only and does not constitute definitive advice
© Appleby Global Group Services Limited 2016