STEVENS&BOLTON

TRANSFERS TO THE UNITED STATES AND THE PRIVACY SHIELD

On 12 July 2016, the European Commission adopted a new legal structure for transferring data from the EU to the United States ("US"), the EU-US Privacy Shield ("Privacy Shield"). This succeeded the Safe Harbour scheme, which was used by many organisations previously as a mechanism for transferring personal data into the US.

Background

Under the eighth data protection principle of the Data Protection Act 1998 ("DPA"), which incorporates the Data Protection Directive 95/46/EC into UK law, personal data must not be transferred outside the European Economic Area ("EEA") unless adequate levels of protection are in place. Whilst certain countries outside the EEA have been found by the European Commission to offer adequate protection, the US has not been one of them.

Therefore, in order to assist, the US put in place the US Safe Harbour scheme which was recognised by the European Commission as providing adequate protection. US undertakings and businesses which signed up to Safe Harbour were able to self-certify their adherence to a series of principles designed to replicate the safeguards of EU law for data protection, thereby enabling the transfer of personal data between the EU and the US in compliance with the eighth data protection principle of the DPA.

However, the Safe Harbour scheme was invalidated in 2015 by a Court of Justice of the European Union ("CJEU") ruling in the case ***Maximillian Schrems v Data Protection Commissioner (C-362/14).*** The case was referred to the CJEU following a complaint by Mr Schrems, in light of Edward Snowden's revelations about the mass surveillance and interception of data by US intelligence agencies, that the US did not ensure adequate protection. The CJEU ultimately found the adequacy decision in respect of Safe Harbour to be invalid and, as a result, Safe Harbour could no longer be legitimately used as a means for transferring personal data to the US. This led to the negotiation and adoption of its successor, the Privacy Shield.

How will the Privacy Shield work?

The Privacy Shield is intended to address the concerns set out by the CJEU in the ***Schrems*** case in relation to Safe Harbour. Under the new framework, the US will be subject to enhanced obligations and it provides for greater levels of involvement and cooperation between the European data protection authorities and the US. The Privacy Shield is intended to safeguard EU personal data that is transferred to the US through various means, such as:

Obligations on US Businesses

Like Safe Harbour, the Privacy Shield is voluntary and is based on a system of self-certification (which will be annual). Organisations that self-certify must make commitments to comply with the data protection

principles that have been agreed between the US and the European Commission, which include various notification and purpose limitation requirements and rules in relation to onward transfers. Those commitments will be monitored and enforced under US law by either the Federal Trade Commission or Department of Transportation depending on the type of business. Human resources data is subject to special rules and organisations that handle such data will be required to cooperate with and comply with the advice of any competent data protection authorities in the EU.

Redress Possibilities

Individuals will be encouraged to raise any complaints with the relevant US organisations in the first instance. However, organisations are also required to provide individuals with access to independent recourse mechanisms, such as independent Alternative Dispute Resolution, free of charge. To ensure that complaints are dealt with expeditiously, organisations will be obliged to respond to complaints within 45 days of receipt and the US Department of Commerce will need to respond to complaints referred to it by European data protection authorities within 90 days. Unresolved disputes that meet certain criteria may be dealt with under a special arbitration procedure.

US Government Access

The US has given the European Commission written assurances that EU citizens will not be subject to indiscriminate surveillance and that the collection and use of EU personal data will be subject to limitations, safeguards and oversight mechanisms. An ombudsperson, who will be independent from the intelligence agencies, will be appointed to deal with individual complaints relating to surveillance activities and confirm either that relevant US law has been complied with, or (in the case of non-compliance) that the non-compliance has been remedied.

US organisations have been able to apply to self-certify under the Privacy Shield framework since 1 August 2016. However, organisations seeking to rely on this new mechanism should note that it has been heavily criticised for failing to provide adequate protection and could face a legal challenge in due course.

Therefore, using the Privacy Shield as the sole basis for transferring personal data into the US could carry some risk.

Alternative mechanisms for US data transfers

The Privacy Shield is only one option available to organisations in order to achieve data protection compliance in transfers to the US. Schedule 4 of the DPA provides alternative methods for allowing international data transfers.

Model clauses

The European Commission has approved standard contractual clauses (known as model clauses) as providing an adequate level of protection. After the CJEU invalidated the Safe Harbour scheme, many organisations began using model clauses as the new basis of transfer for personal data to the US. However, the use of model clauses for transfers of personal data has now been challenged by the Irish Data Protection Commissioner due to the same surveillance concerns and is subject to review by the CJEU. Until the CJEU gives its ruling, the option of using model clauses will remain available. However, the ***Schrems*** judgment states "derogations and limitations in relation to the protection of personal data" should apply "only in so far as is strictly necessary", so their use could still be scrutinised by national data protection authorities in individual cases. Time is another key factor to consider when implementing these clauses across a business.

Binding corporate rules

Another option is to adopt binding codes of corporate conduct, known as binding corporate rules ("BCR") to create rights for individuals, which can be exercised before the courts or data protection authorities, and obligations for the company. This option only applies to multinational organisations transferring information outside the EEA but within their group of entities and subsidiaries. BCRs must be approved by all the relevant European data protection authorities who will co-operate with each other in assessing the standard of your rules. BCRs can be complex, costly and time consuming to implement and therefore will not be suitable for all companies.

Consent

Personal data can be transferred outside of the EEA by relying on the individual's consent, which should be given clearly and freely and may later be withdrawn by the individual. Consent may cause some practical difficulties for organisations in terms of how consent can be collected, what happens if some individuals refuse consent and whether it would be possible to transfer only the data which has been consented to. It is worth noting that the ICO has commented that consent is unlikely to provide an adequate long-term solution to repeated transfers or ones that arise from a structural reorganisation.

Derogations

The data protection rules also include derogations under which personal data can be transferred outside the EEA on the basis of things such as performance of the contract, important public interest grounds or vital interests of the data subject.

Self-assessment of adequacy

In the absence of a European Commission decision on adequacy, organisations are permitted to rely on their own adequacy assessments. An organisation may therefore carry out its own assessment and satisfy itself that there will be an adequate level of protection – albeit this may not provide the same degree of legal certainty as the mechanisms set out above and any decision to proceed with a transfer based on a self-assessment of adequacy could be open to challenge.

It may be that a combination of the above options is used to ensure compliance with the data protection principle, depending on the type of organisation or data in question.

Transfers in light of the General Data Protection Regulation

The General Data Protection Regulation ("GDPR") will start to apply to EU member states from 25 May 2018 and restricts transfers of personal data outside the EU. Even if the UK leaves the EU and the GDPR does not apply directly in the UK, it is likely the GDPR will be replaced with alternative equivalent legislation. In addition, many UK organisations would continue to fall within scope because of its broad territorial application.

The GDPR offers various methods for transfers, including using existing measures such as binding corporate rules and model clauses (although, in light of the existing legal challenges and the need to reflect the enhanced standards in the GDPR, these may look different to the existing model clauses) or complying with approved codes of conduct and certification schemes issued under the new regime. The ease of use and efficacy of these various methods for organisations will become clearer once the GDPR has been implemented.

If you would like to read about the GDPR more generally and about the potential impact of Brexit on its implementation in the UK, please see our briefing note.

FIND OUT MORE

For further information about any of the issues raised in this guide, please contact:

BEVERLEY FLYNN
Commercial Partner &
Head of Data Protection
+44 (0)1483 734264
beverley.flynn@stevens-bolton.com

GARY PARNELL
Commercial Partner
+44 (0)1483 734269
gary.parnell@stevens-bolton.com

Tel: 01483 302264
Fax: 01483 302254
www.stevens-bolton.com