Privacy Shield arrangement enables EU-US data sharing

18 JULY 2016

Kenneth Mullen
PARTNER | UK

CATEGORY:
ARTICLE

The EU Commission has now formally adopted the EU-US Privacy Shield arrangement for the legal transfer of personal data from the EU/EEA to the US.

In parallel moves, the US Department of Commerce has announced that it will be accepting new applications from US companies seeking to self-certify under the Privacy Shield program from 1 August 2016. For more information, click here.

The Privacy Shield is the long-awaited replacement to the 'Safe Harbor' mechanism that was struck down by the European Court in October 2015 in the *Schrems* case brought in the wake of the Edward Snowden affair and concerns about US government surveillance of EU citizens' private data.

While the initial draft Shield was agreed at intra-governmental level in February 2016, extra protections have since been added following criticism from a number of European privacy regulators, leading to the EU Commission ruling on July 12 that the Shield is now regarded as 'adequate'.

Like the Safe Harbor the new Privacy Shield provides a mechanism for US businesses to voluntarily certify compliance with a framework of EU-style privacy principles with the US Department of Commerce. The effect of signing up should mean that when importing personal data from the EU/EEA, Privacy Shield participants will have automatic assurance that they meet European data protection law standards.

New features of the Privacy Shield include the following:

Information about data processing: participant organizations must publish a declaration of commitment to comply with the Privacy Shield principles in privacy policies, enforceable under US law, as well as a link to the Department of Commerce's Privacy Shield website and complaint submission form.

Free and accessible dispute resolution: a participant must respond to individual complaints within 45 days and must provide, at no cost, an independent recourse mechanism. Participants must also commit to binding arbitration at the individual's request to address any complaint that has not been resolved by other mechanisms.

Cooperating with the Department of Commerce: participants must respond promptly to inquiries and requests by the Department of Commerce for information relating to the Privacy Shield Framework.

Maintaining data integrity and purpose limitation: participants must limit personal data use to the information relevant for the purposes of processing and must comply with a new data retention principle.

Transferring data to third parties: when transferring data, participants must comply with 'notice and choice' principles and enter into a contract with any third-party data controller that provides that such data may only be processed for limited and specified purposes consistent with the individual's consent and that the recipient will provide protection for that data consistent with Privacy Shield principles.

The Shield establishes an ombudsperson in the US State Department who will address complaints from EU citizens. The US government has also agreed to limit its access and use of personal data, and the European Commission will cease to challenge the participant organizations' transfer of data to the US.

Businesses should note that, despite European Commission endorsement, the Privacy Shield does not necessarily prevent national regulators in the EEA challenging transfer of data. In addition the Privacy Shield has been criticised by digital rights activists and within the European Parliament for not restricting the US government's collection of EU data. It is therefore possible that a legal challenge will be brought against the EU Privacy Shield in the months to come.

Following the demise of Safe Harbor under the Schrems ruling last year, many US-based organisations who previously benefitted from the regime adopted alternative mechanisms to facilitate legal transfers of personal data from Europe. Probably the most common method has been the adoption of Model Contract Clauses (Model Clauses) between the EU data exporter and US data importer, based on an EU approved standard form contract.

We expect that many organisations may elect to continue with the Model Clauses as their preferred mechanism until the Privacy Shield has had time to bed in. Like Safe Harbor before, certification with the Department of Commerce is only open to US organisations that are subject to FTC or Department of Transport jurisdiction. Banks, credit unions and investment institutions, telecommunications carriers as well as many insurance companies, not-for-profits and other organisations that are not under the FTC/DOT watch remain ineligible.

At the same time with Model Clauses themselves under threat of a pending legal challenge launched by the Irish Government, the Privacy Shield should be seriously considered, in particular by organisations who may have previously been certified with the Department of Commerce under Safe Harbor.

Lastly in relation to US companies with UK data processing operations, clearly Brexit may be an additional consideration. However, certainly for the foreseeable future, the UK is still subject to decisions of the EU Commission in respect of data exports to the US and we recommend organisations treat export of data from the UK as being no different from elsewhere in the EEA/EU.

For more information place contact Kenneth Mullen.

Authors

Kenneth Mullen

PARTNER | LONDON

Intellectual property and technology

+44 20 7597 6189

kenneth.mullen@withersworldwide.com