INTRODUCTION
The Privacy Shield is the new framework for commercial data exchange between the United States and the European Union. A response to the Schrems decision which invalidated the previous Safe Harbor regime, the Privacy Shield aims to restore trust in transatlantic data flows while ensuring the rights of Europeans and providing legal certainty for businesses.

This briefing looks at the Privacy Shield, focusing on how the new framework will operate in practice and the differences between it and Safe Harbor.

SAFE HARBOUR AND THE SCHREMS DECISION
The EU Data Protection Directive (95/46/EC) requires that personal data may only be transferred to non-EEA countries if those countries ensure an adequate level of protection for the personal data. The adequacy of the protection is assessed with regard to the country’s domestic law and the international commitments it has in place for the protection of the private lives and basic freedoms and rights of individuals.

The Safe Harbor Agreement (2000/520/EC) was a voluntary initiative which allowed American organisations that carried out data processing in the EU to self-certify that their processing was undertaken in accordance with the provisions of the EU Data Protection Directive. However, the Court of Justice of the European Union (CJEU) invalidated the Safe Harbor Agreement in the Schrems decision in October 2015. Schrems arose out of a complaint by an Austrian national, Max Schrems, that personal data of his supplied to Facebook in the US by Facebook Ireland was not being processed in accordance with European data protection standards. As the transfers were subject to Facebook’s Safe Harbor certification, and on the basis that Safe Harbor was one of the methods approved by the EU Commission under the Data Protection Directive to validate such transfers, the Irish Data Protection Commissioner had rejected Mr Schrems’ complaint. Mr Schrems appealed this decision to the Irish High Court who in turn referred the matter to the CJEU. His concerns followed revelations by Edward Snowden regarding alleged widespread monitoring of data by US security agencies.

The CJEU decided in favour of Mr. Schrems principally on two grounds. First, it was held that in approving Safe Harbor, the Commission had failed to ensure that the US provided a level of protection of fundamental rights which was equivalent to that guaranteed in the EU. Secondly, the Safe Harbor Agreement potentially deprived data subjects of their rights of access to Data Protection Supervisory Authorities who are vested with the authority to exercise independent oversight of data controllers within their jurisdiction.

The Schrems decision had the practical effect of rendering the Safe Harbor regime invalid. This judgment is part of an increasing body of case law which recognises the protection of personal data as being guaranteed by the Charter of Fundamental Rights of the European Union.

THE PRIVACY SHIELD
The Privacy Shield is intended to be a Schrems-compliant replacement for Safe Harbor. The details of the Privacy Shield were announced by the Commission on 29 February 2016. The Privacy Shield has four key limbs: Obligations on Companies, US Government Access, Redress, and Monitoring.

Obligations on Companies
US companies must register annually to be included on the Privacy Shield list and self-certify that their procedures are in accordance with the seven Privacy Shield principles (Privacy Principles). The Privacy Principles must be satisfied.
in order for processing of personal data to meet the adequacy threshold required by the EU. Organisations must also ensure that their published privacy policies conform to the Privacy Principles and that they are in fact complied with. Employees must be trained on the implementation of the organisation’s privacy policies and compliance must be reviewed periodically in an objective manner.

The seven principles are much the same as those which existed under Safe Harbor and are as follows:

a. **Notice**: Organisations are obliged to provide information to data subjects on a number of key elements relating to the processing of their personal data, such as the type of data collected, the purposes of the processing, the right of access and choice, conditions for onward transfers and liability. Organisations must also make their privacy policies public and provide links to the US Department of Commerce’s (DoC) website and the website of their chosen independent alternative dispute resolution provider.

b. **Choice**: Data subjects may choose to opt out of the transfer of their data to third parties, or the use of their data for materially different purposes than those to which they originally consented, and in respect of sensitive personal data, data subjects must opt in to such processing.

c. **Security**: Organisations creating, maintaining, using or disseminating personal data must take reasonable and appropriate security measures, taking into account the risks involved in the processing and the nature of the data. If an organisation engages a sub-processor, they must ensure that the sub-processor guarantees the same level of protection in accordance with the Privacy Principles.

d. **Data Integrity and Purpose Limitation**: Personal data must be limited to what is relevant for the purpose of the processing, reliable for its intended use, accurate, complete and current. An organisation may not process personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorised by the data subject.

e. **Access**: Data subjects have the right to obtain confirmation from an organisation as to whether the organisation is processing their personal data. This right may only be restricted in exceptional circumstances; any denial of, or limitation to the right of access must be necessary and duly justified, with the organisation bearing the burden of demonstrating that these requirements are fulfilled. Data subjects must be able to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the Privacy Principles.

f. **Accountability for onward transfer**: Any transfer of personal data to third parties may only take place (i) for limited and specified purposes, (ii) on the basis of a contract (or comparable arrangement within a corporate group) and (iii) only if that contract provides the same level of protection as the one guaranteed by the Privacy Principles.

g. **Recourse, enforcement and liability**: Participating organisations must provide robust mechanisms to ensure compliance with the other Privacy Principles and recourse for EU data subjects whose personal data have been processed in a non-compliant manner, including effective remedies.

**US Government Access**

In light of the Snowden revelations, there were strong political motivations on the part of the EU to ensure enhanced protection of the personal data of European citizens. The US government has given the EU written assurances that any access to the personal data of Europeans by US public authorities for national security purposes will be subject to clear limitations and oversight and that there will be no indiscriminate monitoring of personal data of European citizens. The US government has also committed to publishing these commitments on the US Federal Register.

**Redress**

There are a number of avenues for redress under the Privacy Shield. Initially, parties may lodge a complaint with the company itself; the company must respond to such a complaint within 45 days. Companies can also voluntarily commit to comply with the advice of an EU Data Protection Authority (DPA), however in the case of a company which handles European human resources data, the advice of the competent EU DPA must be complied with. Parties may make a complaint to the relevant national DPA, such as the Data Protection Commissioner in Ireland, who will refer it to the DoC, or to the Federal Trade Commission if necessary, to resolve the issue. In order to self-certify for the Privacy Shield, companies must agree to engage an independent dispute resolution body to whom consumers can address complaints. Accordingly, there is an alternative dispute resolution procedure which may be utilised. Finally, and as a last resort, there is also the possibility of arbitration by the Privacy Shield Panel, which can take binding decisions against US self-certified companies.

In terms of data accessed by US national security agencies, the Privacy Shield has a number of mechanisms to allow Europeans challenge perceived unlawful usage of personal data by US authorities for national security purposes. The agreement provides for an Ombudsperson in the Department of State who will be independent of security agencies. The Ombudsperson must inform a complainant whether their complaint has been properly investigated and the relevant law complied with, or in the event of non-compliance, that the breach has been remedied. The US Judicial Redress Act is a further avenue for complainants. When it is commenced, it will grant Europeans access to the US courts.
system to bring civil actions against US government agencies for breaches of the Privacy Act 1974, which established principles relating to the limits which must be observed by security agencies dealing with personal data.

Monitoring

The Privacy Shield provides for an annual joint review mechanism which will allow the US and EU authorities monitor its efficacy. The joint review will have significant regard to the access by security agencies to European personal data.

HOW WILL THE PRIVACY SHIELD WORK IN PRACTICE?

The DoC will have a dedicated website listing the certification criteria that must be met. The DoC will also maintain a public register of organisations that are included in the Privacy Shield. The register will be updated annually on the basis of re-certification submissions and the withdrawal or removal of organisations from the Privacy Shield.

Organisations will be removed from the Privacy Shield for persistent failure to comply with the Privacy Principles. In the case of an organisation being removed, the reasons for removal will be made public on a separate register. Organisations that are removed must return or delete the personal data received under the Privacy Shield. In other cases of removal from the Privacy Shield, an organisation may retain such data if it proves to the DoC on an annual basis that it continues to apply the Privacy Principles to personal data received while it was in the Privacy Shield for as long as it retains this data.

THE MAIN DIFFERENCES BETWEEN SAFE HARBOR AND THE PRIVACY SHIELD

The Privacy Shield was negotiated with the decision of the CJEU in the Schrems case in mind. The primary differences between Safe Harbor and the Privacy Shield are the increased recognition afforded to the personal data of Europeans by the US authorities and the increased obligations on US companies arising from that recognition.

The Privacy Shield requires regular monitoring of the processing of Europeans’ personal data by US companies in the US by the DoC and FTC. The annual review of adequacy decisions conducted by the DoC and the Commission, in particular, is intended to act as a guarantee that commitments are being met by all parties. The Commission has stated that commitments for greater enforcement on the part of the US and enhanced sanctions, such as removal from the Privacy Shield, will transform the system from a self-regulating one to an oversight system that is more responsive as well as proactive.

One of the key areas in which the new regime differs from the old is the obligation in respect of the processing of personal data for national security reasons by US intelligence agencies. In particular, the US has promised that there will be an end to indiscriminate monitoring of Europeans’ data by US authorities. It is hoped that this, coupled with the redress schemes available to complainants, will help ensure that the Privacy Shield is compatible with the CJEU requirements laid down in Schrems.

CONCLUSION

It remains to be seen if the new framework meets the Schrems criteria. Campaigners and organisations such as Max Schrems and the Electronic Frontier Foundation have suggested that the Privacy Shield contains numerous exceptions that will essentially facilitate generalised surveillance by US authorities. MEP Jan Philipp Albrecht has commented that the Privacy Shield is “little more than a reheated serving of the pre-existing Safe Harbor decision”. Therefore if the Privacy Shield faces fresh legal challenges, as Mr. Schrems has suggested it will, it might not provide businesses and other stakeholders with the intended stability and certainty.

The Privacy Shield requires a formal decision by the Commission for it to be enacted as law and therefore may be amended pursuant to the comitology system, which allows representatives of the Member States and the EU DPAs to offer their opinions on the proposed new framework. The Privacy Shield however, is a priority of the EU as the trade in transatlantic digital services is worth some $260 billion dollars and as such, it is expected to be in operation by the Commission's target of June 2016.

The Privacy Shield has also been structured so as to be compatible with Chapter V of the EU General Data Protection Regulation, which is expected to come into effect in mid-2018.
FURTHER INFORMATION
For further information or specific advice regarding how the Regulation will impact your business, please contact any member of the Technology and Innovation team or your usual Arthur Cox contact:

JOHN MENTON
HEAD OF CORPORATE
+353 1 618 0543
john.menton@arthurcox.com

ROB CORBET
HEAD OF TECHNOLOGY & INNOVATION
+353 1 618 0566
rob.corbet@arthurcox.com

PEARSE RYAN
PARTNER
+353 1 618 0518
pearse.ryan@arthurcox.com

COLIN ROONEY
PARTNER
+353 1 618 0543
colin.rooney@arthurcox.com

ISEULT MANGAN
ASSOCIATE
+353 1 618 1153
iseult.mangan@arthurcox.com

OLIVIA MULLOOLY
ASSOCIATE
+353 1 618 1160
olivia.mullooly@arthurcox.com

CHRIS BOLLARD
ASSOCIATE
+353 1 618 0649
chris.bollard@arthurcox.com

CLAIRE O’BRIEN
ASSOCIATE
+353 1 618 1124
claire.obrien@arthurcox.com

JOANNE NEARY
ASSOCIATE
+353 1 618 1114
joanne.neary@arthurcox.com

COLM MAGUIRE
ASSOCIATE
+353 1 779 4356
colm.maguire@arthurcox.com

arthurcox.com
Dublin
+353 1 618 0000
dublin@arthurcox.com

Belfast
+44 28 9023 0007
belfast@arthurcox.com

London
+44 207 832 0200
london@arthurcox.com

New York
+1 212 782 3294
newyork@arthurcox.com

Silicon Valley
+1 650 943 2330
siliconvalley@arthurcox.com