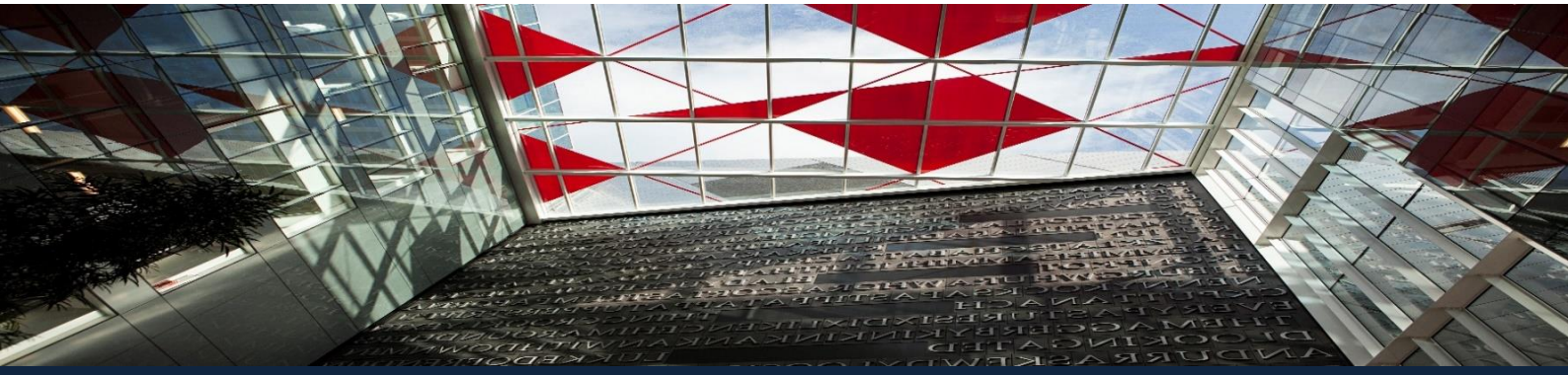

Privacy Source
EU-U.S. Privacy Shield Passes First Annual Review

Privacy Shield, the EU-U.S. data transfer agreement used by over 2,400 companies, recently passed its first annual review. This means the framework will continue in force for at least another year, and provides some much-needed certainty to participating organisations. However the review comes at a time when increasingly difficult questions are being asked about how organisations can uphold privacy principles when transferring data internationally with the review noting a number of areas that need improvement.

Background

Transfers of data between the EEA and U.S. were, until October 2015, governed by what was known as the Safe Harbour framework ("Safe Harbour"). However the Court of Justice struck down the acceptability of Safe Harbour for privacy compliance reasons, following a referral from the Irish High Court in relation to a complaint from privacy campaigner Max Schrems, ruling that it did not comply with a number of EU data protection principles. The EU-U.S. Privacy Shield framework ("Privacy Shield") subsequently replaced Safe Harbour in July 2016.

Privacy Shield specifically lays out more than a dozen privacy principles with which companies must comply in order to rely on Privacy Shield as a means legally to transfer data between the EU and the U.S. The seven primary principles are:

- Notice
- Choice
- Accountability for onward transfer
- Security
- Data integrity and purpose limitation
- Access
- Recourse, enforcement and liability

One of the most important developments within Privacy Shield is the concept of Joint Review. This operates whereby the European Commission and the Article 29 Working Party (WP29) conduct an annual review of Privacy Shield to ascertain whether it is being effective at protecting EU citizens' data.

Ahead of the review in September 2017, the WP29 released a letter outlining what elements would be focused on going forward and specifically identified three main points of concern:

- The language used in the adequacy decision does not oblige organisations to delete data when no longer necessary.
- The U.S. administration does not fully exclude the continued mass and indiscriminate collection of data.
- The workings of the Ombudsperson mechanism.

In addition to noting these points, the WP29 also expressed concern about the U.S. Presidential Executive Order, the Enhancing Public Safety Executive Order (EPSEO), which was signed into law by President Trump on 25 January 2017. Section 14 of EPSEO is ostensibly aimed at enhancing domestic enforcement of U.S. immigration laws and reads: "*Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents*

from the protections of the Privacy Act regarding personally identifiable information."

MEP Jan Philipp Albrecht, the European Parliament's rapporteur on data protection regulation subsequently urged the EU Commission to suspend Privacy Shield in the wake of EPSEO being issued.

In response, a spokesperson for the EU Commission released a statement which noted that *"the U.S. Privacy Act has never offered data protections rights to Europeans"* and further clarified that the EU-U.S. Privacy Shield does not rely on the protections under the U.S. Privacy Act. However, the statement concluded by stating that the EU Commission was *"following closely any changes in the United States that might have an effect on European's data protections rights."*

National Security Guarantees

The WP29 identified two major concerns in the area of national security guarantees. First was the question as to why "*massive and indiscriminate data collection is not fully excluded by the U.S. authorities*" and the second concern is that the "*powers and position of the ombudsperson have not been set out in [much] detail".*

With regard to the first concern, the U.S. provided the EU with clarifications that the access to personal data by U.S. public authorities for law enforcement and national security purposes will be subject to clear limitations, safeguards, and oversight mechanisms. Additionally, the Office of the Director of National Intelligence (ODNI) has clarified that techniques for bulk collection of data that were revealed in 2013 to have been used by the National Security Agency (NSA), could only be used under very specific preconditions and would need to be as focused as possible. In January 2014, President Obama issued the Presidential Policy Directive 28 (PPD-28). PPD-28 states "*privacy and civil liberties shall be integral considerations in the planning of U.S….intelligence activities*." Although PP28 has no enduring legal basis, it can be used to provide interpretive assistance and encourages intelligence agencies to form internal policies that prohibit the collection of data where it could be said to violate privacy and civil liberties.

Nevertheless European Authorities remained unconvinced and in an April 2016 opinion the WP29 stated "*there are indications that the U.S. continue to collect massive and indiscriminate data, or at least do not exclude that they may still do so in the future."* Additionally the WP29 pointed out that although PPD-28 states that targeted data collection should be "*as tailored as feasible*", even this type of restricted data collection could still be considered significant as the Commission's adequacy decision sets out that the "*intelligence community elements must sometimes collect bulk signals intelligence in certain circumstances*".

Furthermore, soon after EPSEO was announced concerns emerged that it could be seen as a direct contradiction to PPD-28 as the language around limiting the exceptional use of bulk collection of data to six national security purposes (counter threats from espionage, terrorism, weapons of mass destruction, threats to cybersecurity or the Armed Forces, or transnational criminal threats) appeared to be considerably broad and do not appear on their face to impose any substantial restrictions on U.S. intelligence surveillance practices. Accordingly Commissioner Jourová indicated that the Commission would be closely following the debate around reform of section 702 of the United States Foreign Intelligence Surveillance Act (FISA) (aimed at targeting communications of non-U.S. persons located outside the U.S.) and how this could affect Europeans data in the light of EPSEO.

The Ombudsperson and Other Remedies

In determining that Safe Harbour was deficient in the case of *Schrems v Data Protection Commissioner C326/14* the European Court of Justice (ECJ) focused on what it viewed as a lack of effective redress for EU individuals who might be aggrieved by the processing of their data by a Safe Harbour-certified organisation. While Privacy Shield retains the independent recourse mechanism to resolve issues, it is something to which certifying organisations must subscribe. Additionally, the recourse mechanism must be impartial, readily available and free for the individual. Privacy Shield also explicitly recognises the possibility of damages and states that both Privacy Shield organisations and the independent dispute resolution body must respond to an individual's complaint within 45 days.

Local data protection authorities (DPA) can also pursue complaints on an individual's behalf. After an individual reports an issue to the relevant DPA, then that DPA can undertake to raise the matter with the U.S. Department of Commerce. The U.S. Department of Commerce and the Federal Trade Commission (FTC) are then under an obligation to investigate and resolve all complaints forwarded to them by a DPA.

As a last resort, an individual can invoke binding arbitration for complaints that are left unresolved. The decision panel will consist of a pool of twenty arbitrators designated by the European

Commission and the Department of Commerce who will have the authority to impose individual-specific, non-monetary, equitable relief to remedy non-compliance with the Privacy Shield (including access, correction, deletion or return of the individual's data in question). The panel may not award damages, costs, fees or other remedies, and each party must bear its own legal fees.

For national security related complaints, a newly created Ombudsperson will handle and solve complaints or enquires raised by EU individuals and be independent from the U.S. intelligence community. Individuals will be informed by the Ombudsperson if their matter has been properly investigated and whether U.S. law has been broken and if so, whether this has since been remedied.

Privacy Shield builds on the original non-compliance consequences under Safe Harbour. On top of the standard consequence of enforcement by the FTC or the U.S. Department of Transportation, there is now a new rule to make public any Privacy Shield related sections of any compliance or assessment report submitted to the FTC. The ability for EU citizens to achieve damages under the recourse and DPA mechanism has been welcomed as a major area of improvement from Safe Harbour.

Nevertheless, there remained a concern around the position of the Ombudsperson mechanism as operating under the U.S. Secretary of State and whether it could be considered adequately independent from the intelligence community (which is required under the definition of an impartial tribunal under Article 47 of the EU Charter of Fundamental Rights). While the WP29 decided that, in keeping with the doctrine of equivalence, an initial judgment regarding the Ombudsperson would be withheld until it could rule conclusively on the overall effectiveness of that office, they have expressed concern on specific elements such as the lack of clarity around the Ombudsperson's investigatory powers and the extent to which it will be capable of making orders of non-compliance. The WP29 also expressed concerns that some of the proposed remedies could not be said to be open fully to EU citizens (for instance EU citizens cannot challenge warrants or subpoenas by invoking the Fourth Amendment of the U.S. Constitution). The draft adequacy decision on the EU-U.S. Privacy Shield (published by the EU Commission) also specified that non-U.S. persons can benefit indirectly though the protection afforded to the U.S. companies holding the personal data that would be subject to the requests. However, the WP29 noted that this does not allow individual citizens to mount a challenge themselves, and means they must instead rely on the relevant company to assert their rights.

In an article for the Irish Times published on 12 July 2016 (the same day as Privacy Shield came into force) Max Schrems and EU MEP Jan-Philipp Albrecht argued that the rules for legal redress are "*rather complex*" and do not *"[guarantee] that the person responsible for oversight will be empowered to actually review the practices of any company*". Schrems and Albrecht also echoed the concerns as to the independence of the Ombudsperson and that judging from EPSEO it appears that the U.S.*"will continue to collect personal data stemming from Europe in bulk*."

Onward Transfers

Previously known as the Onward Transfer Principle under Safe Harbour, the new accountability rules for onward transfers add more requirements for transfers to third parties than were previously explicitly required. In addition, a distinction is made between when the recipient is using the information for its own purposes, that is, acting as a data controller, or when acting as a service provider, that is, a data processor.

Under Privacy Shield, the transferring organisation is now required explicitly to enter into a contract with the third-party data controller. There are two exceptions to this contractual requirement:

- It is not required when transferring a small amount of employee personal data (e.g. what would be used in booking a hotel or a flight.)
- A contract is not required when transferring data between a group of companies under common control when there are binding cooperate rules that ensure the continuity of protection of personal data.

Organisations must meet a host of requirements that includes ensuring relevant contracts contain provisions:

- Complying with the principle of purpose limitation (including notice and choice principles), i.e. the data will be used only for a limited and specified purpose.
- Ensuring that any agent provides the same level of protection as required by the Privacy Shield's principles, and stopping and remediating unauthorised processing.

A summary or a representative copy of the relevant privacy provisions of an organisation's contract with a relevant agent must also be provided to the Department of Commerce upon request.

However the WP29 also raised a number of concerns relating specifically to onward transfers:

- **Accountability:** The WP29 has noted that certain eligible recipient countries were not limited to ones that had Privacy Shield laws. This means that even if a contract enforced certain rules for enshrining Privacy Shield principles, the law of the third country, for example, could allow for public access to personal data for use in surveillance.

- **Lack of reference to the Purpose Limitation Principle:** The WP29 has pointed out that there are references to how data should be kept only for a legitimate purpose and for the time that it is needed, however there is no explicit reference for the need to delete data. In the context of onward transfers the WP29 argues that the lack of this statement makes it unclear that one may not process data for an incompatible purpose. The WP29 note that this is one of the most critical points that has not been implemented.

- **Intra group transfers exception:** The WP29 stated it believes the exception is too vague and the use of the words *"other intra group instrument"* gives rise to the possibility that the transfers could be done under a non-binding agreement.

- **Limited purposes loophole:** The WP29 has said that the section on accountability of onward transfers allows transfers to take place only on the basis that the data are transferred for limited and specified purposes to third parties acting as agents but does not state that those purposes have to be the same as the purpose for which the data were collected originally or in line with the instructions of the controller.

- **Agent assumption:** The WP29 noted that current conditions on onward transfers are built on the assumption that the Privacy Shield organisation acts as a controller and therefore can decide on the possible intervention of any third party agent. However, this would prevent the EU controller from using its control capacities.

Many of the WP29 concerns were also echoed by Max Schrems and Jan-Philipp Albrecht who argued in their Irish Times article that the purpose limitation principle is too broad as it allows the sharing of data for generic purposes such as "*for all services we may provide to you and others*".

First Annual Review

Against this backdrop, the first annual review of Privacy Shield was keenly awaited, not least by the 2,400-odd companies which had become Privacy-Shield certified in the period since the framework's launch in 2016. In order to conduct the review, the EU Commission collected evidence and feedback on the implementation and functioning of the Privacy Shield framework from relevant stakeholders including the Privacy Shield-certified companies themselves, the European data protection authorities, and the U.S. authorities. The EU Commission's Report (the "Report") published on 18 October 2017 examined all facets of the administration and enforcement of the Privacy Shield, including commercial and national-security related matters and wider U.S. legal developments. Overall the Report found that Privacy Shield continues to ensure an adequate level of protection for the personal data transferred from the EU to participating companies in the U.S.

First Annual Review - Positives

Positives outlined in the Report include the following:

- The U.S. authorities are deemed to have established the necessary structures and procedures to ensure the correct functioning of the Privacy Shield (including new redress possibilities for EU individuals).
- Complaint-handling and enforcement procedures have been set up, and there is increased cooperation between the U.S. authorities and the European data protection authorities.
- The self-certification process is functioning well.
- Relevant safeguards remain in place on the U.S. side with regard to personal data accessed by U.S. public authorities for national security purposes. (In this regard, the Report notes that the upcoming debate regarding the re-authorisation of Section 702 of FISA affords a unique opportunity for enhancing and strengthening the privacy protections present in FISA.)

First Annual Review- Recommendations

The Report also makes some recommendations to further improve the functioning of the Privacy Shield including:

- More proactive and regular monitoring of organisations' compliance with their Privacy Shield obligations by the U.S. Department of Commerce is required.
- Regular searches should be conducted by the U.S. Department of Commerce for organisations making false claims about their participation in the Privacy Shield.
- Greater awareness-raising for EU individuals about how to exercise their rights under the Privacy Shield (especially with regard to how to lodge complaints) is necessary.
- Closer cooperation is needed between privacy enforcers, i.e. the U.S. Department of Commerce, the Federal Trade Commission, and the European data protection authorities to develop guidance for companies and enforcers.
- The protection for non-U.S. citizens offered by PPD-28 should be enshrined as part of the ongoing debate on the reauthorisation and reform of Section 702 of FISA.
- A permanent Privacy Shield Ombudsperson should be appointed as soon as possible, and the empty posts on the Privacy and Civil Liberties Oversight Board should be filled.

Next Steps

The Report will be sent to the European Parliament, the Council, the WP29 and the U.S. Authorities. The Commission will work with U.S. Authorities to implement the recommendations of the Report over the coming months and will continue to closely monitor the functioning of the framework, including the U.S. authorities' compliance with their commitments.

In a statement, the WP29 has said that while it was consulted on the Report it intended to conduct its own analysis and publish its own report in November 2017. This WP29's report is eagerly awaited particularly given its previous concerns about aspects of Privacy Shield.

Conclusion

The Report's finding that Privacy Shield is an adequate method to transfer personal data from the EU to the U.S. provides some much-needed certainty to organisations which have either already self-certified under Privacy Shield or which intend to certify in the near future. However, given the Report's recommendations, these organisations should expect greater enforcement efforts from both U.S. and EU regulators in the future.

November 2017


David Cullen
Partner
T +353 1 639 5202
david.cullen@williamfry.com


Leo Moore
Partner
T +353 1 639 5152
leo.moore@williamfry.com


John Magee
Partner
T +353 1 489 6532
john.magee@williamfry.com


John O'Connor
Partner
T +353 1 639 5183
john.o'connor@williamfry.com