Cooley

Data Privacy Q&A: EU-US Privacy Shield

March 3, 2016

At the start of February, the European Commission announced it had finally struck a deal with the US Department of Commerce on Safe Harbor's replacement. Read our initial thoughts. Below, we address some of the key questions organisations are asking about the Privacy Shield.

1. Why do we need a Privacy Shield?

Short answer: Think of it like sun cream - a necessary layer of protection for EU personal data when travelling in the US.

Long answer: Under European Data Protection Law, the transfer of personal data outside of the European Economic Area ("EEA") is prohibited without ensuring that the non-EEA country (referred to by the Commission as a "third country") receiving personal data has adequate protection for such data. There are a number of options to ensure that personal data is protected internationally, including express consent, Model Clauses and Binding Corporate rules, but the least laborious for businesses is where the European Commission has adopted an "adequacy decision" in respect of a particular country, which means that the relevant country ensures an adequate level of protection by reason of its domestic law and international commitments.

The US did not and does not pass this test. Previously, however, the Safe Harbor framework allowed companies to self-certify that they complied with a set of principles and in doing so, were permitted to receive personal data from the EEA – or, put another way, it was possible for personal data to be transferred outside of the EEA to the US. The Edward Snowden revelations a few years ago cast serious doubt on the extent to which Safe Harbor protected EU citizens' data and the ensuing debate ultimately culminated in the framework's invalidation by the European Court of Justice ("CJEU") in October 2015. Read more about the invalidation. Data flow forms an essential part of cross-Atlantic trade and considering the value of EU-US trade relationship, is it is no wonder both parties dedicated significant time, money and effort into the new deal. The Privacy Shield is basically an "upgraded" Safe Harbor, under which the Commission has declared the US meets its adequacy test.

2. What is it?

Short answer: Principles and Promises.

Long answer: The Privacy Shield draft adequacy decision is made up of 7 core and 16 supplemental Privacy Principles as well as additional official representations and commitments (in the form of signed letters) by various US authorities, including Secretary of State John Kerry, Secretary of Commerce, Penny Pritzker, the Federal Trade Commission ("FTC") and the Office of the Director of National Intelligence, amongst others. The Principles aim to reflect the core principles of EU data protection legislation and are entitled accordingly – for example, the "Notice Principle", "Choice Principle", "Security Principle" and "Access Principle". They are essentially criteria each self-certifying organisation must meet, whilst the representations and commitments constitute the promises the US is willing to adhere to in order to maintain the adequate level of protection the European Commission requires.

3. What's different?

Short answer: Quite a bit.

Long answer: The Privacy Shield has had to take into consideration the flowing from the Snowden allegations, the Commission's 2013 requirements and the CJEU's October decision. The Commission breaks down the Shield into four parts:

1. **Commercial Sector** – the Privacy Shield will implement stronger obligations on US companies to protect EU personal data accompanied by stronger monitoring and enforcement via oversight mechanisms, sanctions and tightened conditions for onward transfers to companies' partners.
2. **US Government** – unlike before, the US government has provided written assurances that it will employ and maintain clear safeguards and transparency obligations, for example that any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms.
3. **Redress** – several new mechanisms will be on offer to the EU citizens: directly with the company, in which case the company must reply to the individual within 45 days; free alternative dispute resolution, which will be available via telephone or video conference; to national data protection authorities ("DPAs"), which will work with the US Department of Commerce and FTC to resolve the complaint; or to the newly formed Privacy Shield Panel, via an arbitration mechanism to ensure an enforceable decision.
4. **Monitoring** – the Joint Annual Review will monitor the functioning of the Shield, including, crucially, access to data for law enforcement or national security reasons. The Commission and the US Department of Commerce will conduct the review, with assistance from US national intelligence experts and European DPAs. The Commission will also hold an annual privacy summit and issue a public report to the European Parliament and the Council.

4. Is it any better?

Short answer: Ask the CJEU.

Long answer: The global security landscape has changed and some argue has improved in recent years. The Commission seems happy with the measures the US is taking to alleviate its concerns around disproportionate access to personal data for national security, public interest and law enforcement exceptions, such as Presidential Policy Directive 28, which confines the use of bulk data collection for intelligence operations to six national security purposes (detect and counter threats from espionage, terrorism, weapons of mass destruction, threats to the Armed Forces, or transnational criminal threats) in order to better protect privacy of all persons, including non-US citizens. It also includes the addition of an Ombudsperson within the Department of State, independent from national security services. However, all of this remains subject to the scrutiny of the Article 29 Working Party which is made up of the national DPAS and ultimately, the CJEU, which will undoubtedly receive a selection of test cases in the coming months.

5. Who is in charge?

Short answer: Who knows?

Long answer: There are many players in the Privacy Shield team and the **US Department of Commerce** is the captain. It has committed to most of the compliance administration requirements such as receiving, reviewing and resolving complaints, monitoring and verifying that companies' privacy policies are in line with the Privacy Shield principles, maintaining an updated list of Privacy Shield members and not only removing those that have left, but ensuring those ex-members continue to apply its principles to personal data received when they were in the Privacy Shield, for as long as they continue to retain them.

The FTC is also a key player having committed to work closely with the DPAs to provide enforcement assistance by prioritising referrals from EU DPAs, the Department of Commerce, privacy self-regulatory bodies, and independent recourse mechanisms. It

has also undertaken to establish a dedicated point of contact at the FTC and standardized process through which EU DPAs can refer complaints. A European citizen's "home" **DPA** will continue to be a European citizen's first port of call for a complaint, which will refer the complaint to the Department of Commerce or other appropriate body. The newly created **Ombudsperson** mechanism will handle and resolve complaints or enquiries raised by EU individuals if they fear that their personal information has been used in an unlawful way by US authorities in the field of national security. Where a complaint is not resolved, arbitration is the last resort. Finally, the **Privacy Shield Panel** offers a dispute resolution mechanism that can issue binding decisions against US self-certified companies – and let us not forget the **CJEU** which is of course, still in the mix.

6. What are the practical implications?

Short answer: None for now, but watch this space.

Long answer: Remember the actual text of the Privacy Shield is yet to be formally reviewed and accepted by the Article 29 Working Party, the European Council and the CJEU. US companies interested in self-certifying will have to register to be on the Privacy Shield List and self-certify on an annual basis that they meet the requirements. US companies will also be compelled to display a privacy policy on their website and to respond to complaints from individuals promptly as well as cooperate with European DPAs. EU citizens are granted more transparency and protection under the Shield - EU subsidiaries of US companies and EU companies transferring personal data to the US would be well advised to carefully check their method of transfer. For now, companies on both sides of the Atlantic whose businesses involve a transfer of data from the EEA to the US can, provided they have appropriate alternative mechanisms in place, sit tight until Europe's final checks are complete.

Please contact Cooley's London Privacy & Data Protection team, which is led by partners Ann Bevitt, Mark Deem and Sarah Pearce to clarify options in light of the ruling and practical alternatives to suit your business needs. They offer multi-disciplinary depth and breadth of experience to clients in data protection, privacy by design, data breach management, incident response, breach preparedness, and related litigation, especially in large breaches and those with multi-national issues.

Key Contacts

Ann Bevitt London	abevitt@cooley.com +44 (0) 20 7556 4264

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090