The EU-US economic relationship is the largest bilateral trade relationship in the world, with trade flows valued at over $1 trillion per year. Personal data transfers constitute an essential element of the transatlantic relationship. The legal invalidation of the so-called Safe Harbour arrangement, which provided a framework for transatlantic data transfers, caused major turmoil in recent months and put a strain on the EU-US relationship.

In the absence of the Safe Harbour, companies transferring data from the European Union to the United States face legal uncertainty and possible enforcement and compliance actions throughout EU Member States. Following the judgment which struck down the Safe Harbour, EU national data protection authorities agreed to assess the alternative data transfers tools (Binding Corporate Rules and Standard Contractual Clauses) and potentially take all necessary actions, including coordinated enforcement, should the EU and US fail to arrive at a new transatlantic data transfers framework.

On 2 February 2016, the European Commission announced that a deal with the United States on a new framework for transatlantic data transfers had been reached. The EU-US Privacy Shield arrangement aims to address loopholes identified in the Safe Harbour judgment, thus providing guarantees that EU citizens’ data continue to be protected once transferred to the United States.

Welcomed by industry but others, including privacy campaigners and several Members of the European Parliament questioned the solidity of the new deal, hinting that should the Privacy Shield be brought in front of the Court of Justice of the European Union, it could get struck down in the same manner as its predecessor.

In this snapshot, FTI Consulting provides an analysis of the different steps that led to the establishment of the EU-US Privacy Shield and an overview of the latest developments which will impact on companies transferring data across the Atlantic going forward.
The 1995 EU Data Protection Directive (which is currently still in force, however new rules recently agreed on shall come into force in 2018) stipulates that EU citizens' data can only be transferred outside the EU when an adequate level of data protection is guaranteed. On the basis of the Directive, in July 2000 the European Commission adopted a decision recognising the Safe Harbour Privacy Principles issued by the US Department of Commerce as providing adequate protection for personal data transfers from the EU to companies in the US, despite the lack of a general data protection law in the US.

Over 4,000 organisations subject to the jurisdiction of the US Federal Trade Commission or US air carriers and ticket agents subject to the jurisdiction of the US Department of Transportation which were eligible to participate in the Safe Harbour signed up and thus able to freely transfer personal data to the US. The functioning of the Safe Harbour relied on commitments and self-certification of the signatories; with the US Federal Trade Commission responsible for the enforcement.

On 6 October 2015, the Court of Justice of the European Union (CJEU) delivered its judgment in Case C-362/14 (Maximillian Schrems v Data Protection Commissioner) declaring the European Commission’s decision on Safe Harbour invalid.

Although the Safe Harbour’s invalidation was often depicted as a surprise, this was not the case for the European Commission and European Parliament who, following Edward Snowden’s revelations about the surveillance activities of the US intelligence services, pointed to the agreement’s shortcomings since 2013.

I have been very clear from the start of this mandate: we want to be sure that when Europeans’ personal data is sent to the US, the data continues to be protected. Secure and open exchange of data is very important in our digital world.

Andrus Ansip, European Commission Vice-President for the Digital Single Market

Political context and timing: From Snowden to Schrems

The safety of data transferred under the Safe Harbour started to be questioned in the wake of Edward Snowden’s revelations. In July 2013, the then EU Justice Commissioner Reding announced that the European Commission was working on a solid assessment of the Safe Harbour. Alongside the Commission’s assessment, the European Parliament’s Civil Liberties Committee launched an inquiry on electronic mass surveillance of EU citizens which led several political groups, including the centre-right European People’s Party and liberal ALDE group, to call on the European Commission to suspend the Safe Harbour.

Concluding that the functioning of the Safe Harbour was deficient, in November 2013 the European Commission presented a list of 13 recommendations designed to improve the framework. The recommendations revolved around four major areas for improvement: transparency, judicial redress, effective enforcement and limitations of access to data by public authorities. The list was used by the Commission as a basis for negotiations with the US on a strengthened framework which were launched in January 2014.

Following Snowden’s revelations, Austrian privacy campaigner Maximilian Schrems lodged a complaint with the Irish Data Protection Commissioner arguing that the law and practice of the United States did not offer sufficient protection against public authorities surveillance of the EU citizens’ data transferred to the US. The Irish Data Protection Commissioner rejected the complaint referring to the European Commission’s Safe Harbour decision which stipulated that, under the Safe Harbour, the United States ensures an adequate level of protection of data transferred. The High Court of Ireland referred the case to the CJEU seeking clarification with regards to a national data protection authority’s entitlement to investigate a complaint alleging that a third country did not ensure an adequate level of protection, even though the adequacy was confirmed by a decision of the European Commission.

Safe Harbour struck down

In its ruling of 6 October 2015 which invalidated the Safe Harbour, the CJEU reiterated the importance of the fundamental right to protection of personal data, including when data is transferred outside the EU. The Court said that the European Commission’s Safe Harbour decision did not contain sufficient findings on the limitations with regards to the US public authorities access to data transferred under that decision and on the existence of effective legal protection against such interference. The Court stated that US requirements related to national security, public interest and law enforcement prevailed over the Safe Harbour, thus making US companies bound to disregard the Safe Harbour’s protective rules where they conflict with those. The Court also said that a generalised access to the content of electronic communications by public authorities compromises the fundamental right to respect of private life. Likewise, the absence of legal remedies for an individual to have access to his or her personal data compromises the right for effective judicial protection, the Court argued.

The Court held that the existence of a European Commission decision that a third country ensures an adequate level of protection of personal data transferred cannot eliminate or reduce the powers of national supervisory authorities to independently examine whether personal data transfers to a third country comply with the requirements laid down by the EU Data Protection Directive.

EU-US Privacy Shield unveiled

On 2 February 2016, Andrus Ansip, European Commission Vice-President in charge of the Digital Single Market, and Justice Commissioner Věra Jourová confirmed that the European Commission and the US reached an agreement on a new framework for transatlantic data transfers – EU-US Privacy Shield. The EU College of Commissioners backed the political agreement
and mandated Ansip and Jourová to draft an adequacy decision which would bring the agreement to life.

The Commissioners voiced their conviction that the new arrangement provides strong guarantees for the protection of EU citizens’ data, safeguards with regards to the US authorities access to the data transferred, and effective redress mechanisms.

While the final text of the arrangement has not yet been made public, the European Commission highlighted that US companies that transfer data under the new arrangement will commit to strong data processing obligations, to be monitored by the US Department of Commerce and enforceable under US law.

The EU-US Privacy Shield addresses the issue of access to the data transferred by the US public authorities. The European Commission stressed the importance of the commitment made by the US authorities with regards to limitations, safeguards and oversight mechanisms that will apply to US authorities access to data for law enforcement and national security purposes.

“This new framework for transatlantic data flows protects the fundamental rights of Europeans and ensures legal certainty for businesses. The new arrangement lives up to the requirements of the European Court of Justice. It will also be a living mechanism, which will be reviewed continuously to check whether it functions well.”

Věra Jourová, European Commissioner for Justice, Consumers and Gender Equality

The functioning of the Privacy Shield will be subject to an annual joint review by the European Commission and the US Department of Commerce, with the participation of US national intelligence experts and EU data protection authorities.

The Privacy Shield will provide several mechanisms which will allow EU citizens to ascertain their rights if they consider their data has been misused. The redress mechanism will demand greater cooperation from business as they will be required to reply to complaints. Under the new arrangement, EU data protection authorities will work closely with the US Federal Trade Commission to ensure that complaints are investigated and resolved. If a case is not resolved, the arrangement provides for an arbitration mechanism. Furthermore, a new Ombudsman function will be created in the United States to deal with contentious cases in the area of national security.

Before the Shield gets activated...

The Article 29 Working Party (WP29), an umbrella organisation of the European data protection authorities, led by Isabelle Falque-Pierrotin, Chair of the French data protection watchdog (CNIL - Commission Nationale de l'Informatique et des Libertés), cautiously welcomed the EU-US Privacy Shield. Falque-Pierrotin explained that upon receipt of all documents related to the Privacy Shield, the WP29 will assess the new framework, seeking to verify the robustness of its provisions in light of the Safe Harbour judgment. Should the European Commission communicate the documents by the end of February, Falque-Pierrotin expects for the WP29 to announce its final decision in April.

Other data transfers tools – real alternatives or more uncertainty?

While transatlantic data transfers can no longer be based on the Safe Harbour, companies can use other tools to transfer data to the US:

• Standard Contractual Clauses: European Commission provides templates for contractual terms for companies dealing with overseas data processors;

• Binding Corporate Rules: set of rules outlining a company’s policies on international transfers of personal data within the same corporate group.

The WP29 initiated an assessment of the Safe Harbour judgment’s impact on these alternative data transfer tools; the assessment will also encompass the provisions of the EU-US Privacy Shield. Until the publication of its assessment, the WP29 announced that businesses should be using Standard Contractual Clauses and Binding Corporate Rules for data transfers to the US. The WP29 reiterated that any company that still uses Safe Harbour as the basis for data transfers is acting illegally. However, the use of alternative data transfers tools might also prove problematic as it was reported that several consumer groups are ready to file complaints against their use, leaving companies in legal uncertainty as to how to proceed. Furthermore, Maximilian Schrems announced that he had submitted requests to the Irish, Belgian and City of Hamburg data protection authorities to further investigate the use of Standard Contractual Clauses. It remains to be seen whether EU national data protection authorities will coordinate their actions and wait until the final assessment of the Privacy Shield is completed before launching investigations into alternative data transfers tools.

National data protection authorities have the power to suspend data transfers if they do not comply with EU law. Given that enforcement of EU privacy law is done at Member State level, a coordinated approach is essential. However, the common front of the WP29 tends to erode quickly, as some national authorities adopted a tougher stance on the issue of alternative tools only few weeks after the Safe Harbour judgment. For example, on 26 October 2015, Germany’s federal and state data protection authorities announced that they will temporarily stop authorising new data transfers to the US. Johannes Caspar, Hamburg’s privacy regulator, stipulated that companies wanting to avoid legal and political consequences of the Safe Harbour judgment should consider storing personal data on servers located in the EU. In the aftermath of the judgment, several US companies announced their intention to open new data centres in the EU; Amazon announced the opening of a new centre in the United Kingdom before 2017, while Microsoft entered into a new partnership with Deutsche Telekom to store its cloud data in Germany. A push for companies to store data in the EU, although not based on a legal requirement, may have serious financial repercussions. Prolonged uncertainty
about the safety of transatlantic data transfers may also affect a company’s perception among those EU consumers more inclined to choose a provider that stores data in the EU which is generally perceived as safer, despite revelations that several EU Member States also engaged in surveillance activities.

View from San Francisco

If nature abhors a vacuum, commerce abhors uncertainty. The simple truth is that the law of unintended consequences is quite clearly on display here: while the instinct to create mechanisms that provide a set of rules and remedies to govern the use of data is both understandable and admirable, the volume and velocity of modern data flows mean that to suspend one regulatory regime, without having its replacement ready to deploy, can only serve to maximise frustration.

While it might be fairly argued that the fragility of the previous Safe Harbour agreement should have been more evident to US companies (and certainly to those technology giants whose primary business relies on the daily flow of billions upon billions of digital data sets), they simply weren’t. Both US corporations (and the government itself) were caught off-guard by recent events.

This outcome suggests at a certain level there was a lack of cooperation and coordination, whether formal or informal, between the EU and the US on this crucial issue. Sentiment within US commercial circles (which, to be clear, is not the same as data privacy circles) is predicated on a much different view of the necessity of regulations and standards, and current sentiment is now informed by an absence of clear standards.

Frustration on the part of US industry, famously resistant to regulatory constraints, is less a function of the burdens (financial, legal, and otherwise) of compliance with a new and more robust EU data privacy regime, but rather, a function of a lack of clarity upon which to predicate corporate operations.

FTI Consulting would venture that in practical terms, both sides are closer than they think. While the EU might justifiably argue that standards critical to protecting consumers is hardly worth sacrificing for the sake of profit - and in turn their American counterparts wonder why a functional set of existing rules collapsed - there is an immense amount at stake. Both sides, ultimately, seek viable set standards.

But until a clear framework emerges, the options confronting most companies aren’t palatable, or sustainable, from an operational point of view. On the face of it, it is difficult to imagine any of the thousands of multinational corporations for whom data capture, analysis, monetisation and transfer is critical, and who may no longer rely on Safe Harbour rules, to want to have to negotiate and manage thousands (if not millions) of individual bilateral contractual agreements to govern data transfers, especially as future rulings may find them deficient.

The suggestion, similarly, by various EU Member States that a solution to this issue would be to construct new data storage centres within their borders can’t help but feel to many US corporations as a thinly veiled, distinctly modern, form of mercantilism.

Ultimately, commercialism is a form of pragmatism. Despite a short period of turmoil, we expect US companies to embrace any reasonable and clearly defined structure designed to protect the very data that drives the growth of their enterprises.

View from Berlin

The German Government’s discomfort with this issue was evidenced by a recent debate in the Federal parliament. Berlin is extremely reluctant to come up with a clear position on the Safe Harbour ruling at this point in time: no-one wants to alienate the Americans (due to TTIP and the upcoming US elections), in parallel, no-one wants to be seen as weak on consumers’ rights. Instead, there is hand-wringing on an issue which is historically a sensitive one in Germany. So, while expectations are high at EU-level, pressure to find a smooth solution is increasing in Berlin, too. But for now, the government just hopes to stay out of this and leave deal breaking to Brussels.

Conclusion

The EU-US Privacy Shield agreement was broadly welcomed by business community representatives. However, it is not yet clear whether the new framework will provide lasting legal certainty for businesses transferring data from the EU to the US. Commenting on the deal, MEP Jan Philipp Albrecht (Greens, Germany), the European Parliament’s Rapporteur on the General Data Protection Regulation, the EU will soon start implementing, said that the Privacy Shield does not foresee legally binding improvements.

The European Commission will work on drafting the adequacy decision which will bring the new EU-US framework to life. According to Commissioner Jourová, the draft should be ready in the coming weeks. After obtaining the advice of the WP29, and consulting representatives of the EU Member States, the College of Commissioners will adopt the decision. Alongside this process, the US will take the steps necessary to set up the new framework, including the monitoring mechanism and Ombudsman. Once established, the EU-US Privacy Shield should provide long-term legal certainty able to withstand a possible next challenge in front of the Court of Justice of the European Union.
The (un)certain future of transatlantic data transfers

TMT Public Affairs and Strategic Communications team

Charles Palmer
Senior Managing Director - Global Head of TMT
FTI Consulting
200 Aldersgate, Aldersgate Street
London EC1A 4HD
United Kingdom
T: +44 20 3727 1400
Charles.Palmer@fticonsulting.com

Julia Harrison
Senior Managing Director - Managing Partner Brussels
FTI Consulting
Avenue Marnix 23
1000 Brussels
Belgium
T: +32 (0) 2 289 09 30
Julia.Harrison@fticonsulting.com

Robbie Goffin
Senior Advisor - Strategic Communications
FTI Consulting
One Front Street, Suite 1500
CA 94111 San Francisco
United States
T: +1 646 468 9039
Robbie.Goffin@fticonsulting.com

Marzena Rembowski
Director, Head of TMT at FTI Brussels
FTI Consulting
Avenue Marnix 23
1000 Brussels
Belgium
T: +32 476 01 11 00
Marzena.Rembowski@fticonsulting.com

Nikolas Lemke
Director – Strategic Communications
FTI Consulting
Luisenstraße 45
10117 Berlin
+49 (0)30 288 744 241
Nikolas.Lemke@fticonsulting.com

Miroslav Pospisil
Senior Consultant
FTI Consulting
Avenue Marnix 23
1000 Brussels
T: +32(0)2 289 09 32
Miroslav.Pospisil@fticonsulting.com

About FTI Consulting
FTI Consulting Inc. is a global business advisory firm dedicated to helping organisations protect and enhance enterprise value in an increasingly complex legal, regulatory and economic environment. FTI Consulting professionals, who are located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges in areas such as investigations, litigation, mergers and acquisitions, regulatory issues, reputation management and restructuring. The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting Inc., its management, its subsidiaries, its affiliates, or its other professionals, members or employees.

www.fticonsulting.com

©2016 FTI Consulting Inc. All rights reserved.