European Parliament

From Safe Harbour to Privacy Shield

Advances and shortcomings of the new EU-US data transfer rules

IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service
Authors: Shara Monteleone and Laura Puccio
Members' Research Service
January 2017 — PE 595.892

EN

The October 2015 *Schrems* judgment of the Court of Justice of the European Union (CJEU) declared invalid the European Commission's decision on a 'Safe Harbour' for EU-US data transfer. The European Commission negotiated a new arrangement, known as Privacy Shield, and this new framework for EU-US data transfer was adopted in July 2016. This publication aims to present the context to the adoption of Privacy Shield as well as its content and the changes introduced.

PE 595.892
ISBN 978-92-846-0369-5
doi:10.2861/09488
QA-06-16-293-EN-N

Original manuscript, in English, completed in January 2017.

Disclaimer

The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to the Members and staff of the EP for their parliamentary work. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2017.

Photo credits: © vector_master / Fotolia.

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

EXECUTIVE SUMMARY

In the 2015 *Schrems* case, the Court of Justice of the European Union (CJEU) declared the European Commission's 2000 decision on the 'adequacy' of the EU-US Safe Harbour (SH) regime invalid, thus allowing data transfers for commercial purposes from the EU to the United States of America (USA). One of the main concepts on which the reasoning of the Court relies is that of 'equivalence' between the level of protection existing in a third country, and the European data protection system. The Court invalidated the SH adequacy decision as it did not contain any findings regarding the existence in the USA of laws and practice limiting interference to the right to privacy and data protection (e.g. interference by public authorities for security purposes), nor of effective judicial remedies for individuals. Accordingly, says the judgment, laws which establish exceptions (such as enacting measures for security purposes) which can lead to conflict with fundamental rights should lay down clear and precise rules regarding the scope and application of the measure, and minimum safeguards against risk of abuse, including unlawful access and further use of such data. The corollary of this statement is that derogations and restrictions to data protection should be allowed only if strictly necessary. Moreover, whereas the self-certification mechanism for US-based companies can be part of an adequate data protection system, it should be accompanied by effective enforcement and oversight mechanisms.

As a consequence, the SH framework, on which a large number of companies relied, proved insufficient to ensure the high level of protection for EU citizens demanded in EU law. This invalidation of SH created legal uncertainty and the need for a new arrangement. In the meantime, more than 4 000 US companies making data transfers switched to other existing tools, albeit more burdensome and limited, such as Binding Corporate Rules or Standard Contractual Clauses.

Consequently, the European Commission and the USA negotiated in 2016 a new framework for transatlantic exchange of personal data, known as the **Privacy Shield** (PS). This framework had to address the Commission's 13 recommendations, made in 2013, as well as tackle the main concerns raised by the Court in its *Schrems* judgment. Although representing significant improvements compared to SH, some concerns remain to be addressed, failing which the situation of legal uncertainty may not disappear: Privacy Shield may not therefore withstand possible future complaints.

TABLE OF CONTENTS

List of main acronyms used

Article29WP:	Article 29 Working Party (EU)
BCR:	Binding corporate rules
CC:	Contractual clauses
CFR:	Charter of Fundamental Rights (EU)
CJEU:	Court of Justice of the European Union
DoC:	Department of Commerce (USA)
DPAs:	Data protection authorities (EU)
DPD:	Data Protection Directive
EC:	European Commission
ECtHR:	European Court of Human Rights
EDPS:	European Data Protection Supervisor (EU)
FISA:	Foreign Intelligence Surveillance Act
FOIA:	Freedom of Information Act
FTC:	Federal Trade Commission (USA)
GDPR:	General Data Protection Regulation
JDR:	Judicial Redress Act
PCLOB:	Privacy and Civil Liberties Office Board
PS:	Privacy Shield
SCC:	Standard contractual clauses
SH:	Safe Harbour

1. Introduction

On 6 October 2015, in *Schrems* v. *Data Protection Commissioner*, the Court of Justice of the European Union (CJEU) declared invalid the European Commission's decision No 2000/520/EC[1] on the 'adequacy' of the US data protection system (SH), in relation to the transfer of personal data from the EU to the USA. In this judgment, the Court also clarified that the investigative powers of national data protection authorities are not reduced by the existence of a Commission adequacy decision. As a consequence, the SH framework proved insufficient to ensure protection for EU citizens, given the EU legal requirement for respect of a high level protection when data are transferred outside the European Economic Area (EEA). As a result, a new framework for governing transatlantic data flows became urgent.

Recent developments in EU policy and in EU-US relations include a new framework to replace Safe Harbour, the Privacy Shield, and the Commission's adoption of the related adequacy decision on 12 July 2016. These processes, and their implications for businesses, citizens and EU institutions, are explored below.

2. EU policy on data transfer and the Schrems case

2.1. High level of EU data protection and third countries

The European Data Protection Directive (DPD) 95/46/EC[2] (and the General Data Protection Regulation[3] that replaces it from 2018), aims to encourage coherent free movement of personal data while protecting the individual rights of the persons concerned.

A high level of protection is ensured to the extent that data transfers outside the EU/EEA are only allowed if third countries guarantee an **adequate** level of protection (Article 25 of the DPD). The European Commission may find, by adopting an 'adequacy' decision, that a third country ensures an adequate level of protection. Such adequacy shall be assessed 'in light of all the circumstances' surrounding data transfer operations including domestic laws, international agreements and 'the rule of law' in force in the third country in question (article 25 (2) DPD).[4] Therefore, the decision on adequacy involves assessing

---

1 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by SH privacy principles and related frequently-asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441).

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

4 See Data Protection Directive Article 25 (5): 'At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4 [not adequate level]' and (6) 'The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection [...], by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.'

the presence in the third country of a legal framework for data protection giving similar guarantees and redress measures to the European Union.

Box 1 – Procedure for adoption of the 'adequacy decision'

The European Commission assesses the level of data protection in the third country via an examination procedure (following Articles 25(6) and 31(2) of the DPD). The Commission proposal is approved under the new comitology rules, within the Article 31 Committee, made up of representatives of Member States.[5] The committee decision is based upon an opinion issued by national data protection authorities and the European Data Protection Supervisor (EDPS). The Commission can pursue the proposed measure if it obtains a qualified majority in favour of the proposal. The College of Commissioners formally adopts the adequacy decision. The European Parliament and the Council should simultaneously receive information regarding actions taken in committee (right of information), and can request the Commission maintain, amend or withdraw an adequacy decision at any time if it is considered to exceed the implementing powers given to the Commission by the Directive (right of scrutiny).

On that basis, the Commission issued **adequacy decision 2000/520** (hereafter the SH adequacy decision), stating that the 'Safe Harbour' framework, enacted by the US Department of Commerce (DoC), was 'adequate', and allowing personal data transfers from EU to the USA. In particular, the decision allowed companies to transfer data without requiring any specific assessment of the US data protection system, thus simplifying their implementation of EU data protection requirements.[6]

Box 2 – Former Safe Harbour protection

United States data controllers complying with SH principles[7] were considered to offer adequate protection, and the transfer of data to those firms was therefore allowed under article 25 of the Data Protection Directive (DPD). If the data controller outsourced processing activities, it had to ensure data protection safeguards were in place within the contractual obligations with the outsourced firm. Ultimately under SH, the data controller remained legally responsible and accountable for the processing of the data. The SH principles were not compulsory; firms joined them voluntarily. To do so, they issued self-certification stating that they complied with the SH principles. Companies that failed to provide annual self-certification would no longer appear in the list of participants and would no longer be entitled to SH benefits. The validity of self-certifications was verified by the US Department of Commerce (DoC), who also had to maintain the updated list of the firms with valid certifications.[8]

---

[5] See article 5 of the Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ [2011] L 55/13.

[6] For the full list of Commission adequacy decisions, refer to the Directorate-General for Justice website.

[7] Issuance of SH principles and transmission to European Commission, Federal Register 24 July 2000 and 19 September 2000

[8] Telecommunication services were subject to an exception from the Free Trade Commission Act and could therefore not participate in the SH self-certification framework. Transport services participating in the SH were monitored by the Department of Transport.

Monitoring of compliance fell to the Federal Trade Commission (FTC) and only firms under the jurisdiction of the FTC could participate.[9] Indeed, as the SH principles function like promises to customers, failure to comply with such promises triggers a case of unfair and deceptive practices pursuant to section 5 of the Free Trade Commission Act.[10]

The European Commission has recognised the emerging 'inadequacy' of the SH since 2013. In a 2013 review of the SH framework by the Commission,[11] the following issues regarding the monitoring and enforcement of the SH principles were detected: (a) transparency of the privacy policies of SH companies was not always respected, although this is an important feature to ensure enforceability via section 5 of the Free Trade Commission Act; (b) lack of proper follow-up and verification of the validity of SH certification, as well as effective compliance with the principles; (c) limited access to redress mechanisms.

On 6 October 2015, the Court of Justice of the EU (CJEU) declared the SH adequacy decision **invalid**, rendering urgent the need to adopt a new EU-US data-transfer framework.

2.2. Court of Justice of the EU: *Schrems* case and its consequences

In light of Edward Snowden's revelations[12] in 2013 about the US National Security Agency's mass surveillance programmes (e.g. PRISM)[13] and veiled collaboration with internet companies, an Austrian privacy lawyer, Max Schrems, lodged a complaint with the Irish Data Protection Authority (DPA), questioning the lawfulness of data transfer to the USA, on the assumption that all European Facebook subscribers' data are regularly transferred to servers in the USA. In particular, by invoking the investigatory powers of the Irish DPA,[14] Schrems made the claim that US law and practice does not offer adequate protection **against the risks of mass surveillance** to EU citizens (according to

---

9 The FTC is not always the authority responsible. The FTC's primary legal authority comes from section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. Other laws ensure privacy in sectors such as health services, telecommunications or some financial and insurance sectors that are outside the FTC jurisdiction, but are covered by other departments or commissions. For cases brought under the SH Framework by the Federal Trade Commission; see also: C. J. Hoofnagle, Federal Trade Commission Privacy Law and Policy, Cambridge University Press, 2016, on the work of the FTC in data protection.

10 15 US Code §45

11 Communication from the Commission to the European Parliament and the Council on rebuilding trust in EU-US data flows, COM(2013) 846 final, 27/11/2013; communication from the Commission to the European Parliament and the Council on the functioning of the SH from the perspective of EU citizens and companies established in the EU, COM(2013) 847 final, 27/11/2013.

12 E. Macaskill and G. Dance NSA files: decoded, The Guardian, 1 November 2013.

13 On this issue, the European Parliament adopted a series of resolutions in which it has repeatedly called for the suspension of SH and urged the Commission to take immediate action to ensure effective data protection in transfers to the USA; see: European Parliament, Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy; Resolution of 12 March 2014 US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights, and Resolution of 29 October 2015, follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens.

14 The Irish DPA was competent as Facebook's European intermediary is Facebook Ireland. Documents on the different administrative and court proceedings are published by *Europe v Facebook*.

the DPD). The Irish data protection Commissioner rejected the complaint on the grounds that EU-US data transfers relied on the Commission's binding 'SH' adequacy decision.

The case was brought in front of the High Court of Ireland for judicial review, which in turn referred to the CJEU for a preliminary ruling, therefore calling into question the lawfulness of the SH framework under which the transfer occurred.[15] In other words, the Irish High Court asked whether the existence of the SH adequacy decision impedes a DPA investigation on the basis of a complaint.

In the *Schrems* v. *Data Protection Commissioner* ruling,[16] the CJEU met in Grand Chamber, confirmed Advocate General Bot's opinion,[17] and went further than the *Schrems* and Irish Court claims, and indeed, of its own motion, stated that:

1) national DPAs have the power to examine a person's claim (as enshrined by DPD and by the EU Charter of Fundamental Rights (CFR); such power is not reduced by the existence of a Commission adequacy decision;
2) the Commission's findings on the SH voluntary scheme in the adequacy decision were insufficient to ensure that EU citizens' data are protected in the USA;
3) derogations for security purposes should be strictly necessary and proportional.

The Court declared – as the only party entitled to do so – therefore the related Commission adequacy decision to be invalid. The main passages of the judgment are analysed in the following sections.

2.2.1. *DPA powers*

National supervisory authorities are not prevented from investigating the lawfulness of data transfers from the EU to a third country, even if a Commission decision exists on the level of protection provided in that country. As Steve Peers noted,[18] the Court based its conclusion on the powers and independence of those authorities as enshrined in DPD, read in light of the EU CFR, which expressly refers to DPA's role and independence.[19] Analysing this issue within the architecture of the data protection system as regards external transfers, the Court confirmed that while the DPAs are bound by the Commission decision and cannot declare it invalid (only the CJEU has this power, otherwise a fragmentation of EU law would result), they can however investigate a case upon receiving a complaint. Moreover, if the complaint is well-founded, DPAs can bring

---

15 The Irish High Court, by requesting a preliminary ruling from the CJEU, asked the following questions: 'Whether in the course of determining a complaint which has been made to [the Commissioner] that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, [the Commissioner] is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of the [CFR], the provisions of Article 25(6) of Directive [95/46] notwithstanding? Or alternatively may and/or must the [Commissioner] conduct his or her own investigation of the matter in the light of factual developments in the meantime since [Decision 2000/520] was first published?'.

16 Case C‑362/14 *Maximilian Schrems* v. *Data Protection Commissioner*, of 6 October 2015.

17 See Opinion of Advocate General Bot delivered on 23 September 2015.

18 S. Peers, *The party is over: EU data protection law after Schrems SH judgment*, EU law analysis Blog, 7 October 2015.

19 The new Regulation (GDPR) actually enhances these powers and independence (article 51 and following).

this before the national courts, according to national rules, to have the issue referred to the CJEU.[20]

2.2.2. *High level of data protection*

As indicated above, the Court held that the Commission's adequacy decision on SH was invalid because the manner in which interferences with fundamental rights in the USA would be limited to that strictly necessary did not emerge from that decision.

In so doing, the CJEU stressed the need to interpret the requirement of adequate protection under DPD as **essentially equivalent** to that guaranteed in the EU, in line with the Directive's objectives of ensuring a high level of protection that extends to personal data transferred outside the EU (otherwise the same requirement would be easily circumvented).[21] Furthermore, according to the Court, this requirement should be read in accordance with the CFR, which protects rights to privacy (Article 7), to data protection (Article 8) and to effective judicial remedy (Article 47) and which, as noted, entrusts national DPAs with supervisory powers. This also implies a continuous assessment of the rules and practices of third countries in terms of safeguards, as conditions to transfer data: a dynamic assessment, with regular reviews, so that changes in circumstances since the adoption of the decision are taken into account.[22]

Box 3 – The Schrems case: in line with previous Court of Justice of the EU jurisprudence

The *Schrems* judgment forms part of growing and consistent CJEU jurisprudence, stressing the significance of high-level protection of personal data (e.g. the *Google Spain* and *Digital Rights Ireland* cases.)[23] In particular, some aspects discussed in the *Digital Rights Ireland* judgment formed the basis of arguments that the Court later upheld in the *Schrems* case.[24] In *Digital Rights Ireland*, the Court examined the validity of the Data Retention Directive in light of Articles 7, 8 and 11 of the Charter of Fundamental Rights (CFR), and stated that the retention it permitted represented a particularly serious interference with the rights enshrined in these articles (although not sufficiently to affect their essence, as the Directive did not permit the acquisition of the content of the electronic communications). While the objective of the Data Retention Directive (the fight against serious crime) is considered by the Court as legitimate, in order to be a lawfully justifiable limitation of the right recognised in Article 7 CFR, the retention must be strictly necessary.[25]

---

[20] See also A. Azoulai & M. van der Sluis, 'Institutionalizing personal data protection in times of global institutional distrust: Schrems', *Common Market Law Review* 53, p. 1343, 2016.

[21] On the concept of 'extraterritoriality' (and on the need to determine boundaries of the application of EU data protection law) see C. Kuner, 'Extraterritoriality and regulation of international data transfers in EU data protection law', *International Data Privacy Law* (2015), 5 (4).

[22] See S. Peers, who stressed that the Commission's decision was declared invalid in light of the importance of data protection rights in European (that will be affected). See also S. Rodota, 'Internet e-privacy, *c'e' un giudice in Europa che frena gli* USA', La *Repubblica*, 12 October 2015, who stressed that 'Facing a politics curved solely on the economics, are the judges who try to keep alive the Europe of rights.'

[23] C-131/12 and Joined Cases C-293/12 and C-594/12; see also the recent judgment in the joined Cases C‑203/15 and C‑698/15 (*Tele2 Sverige* and *Watson and Others*).

[24] In this sense, E. Ustaran, H. Lovells, The Privacy Shield explained, Part 2, in P*rivacy & Data Protection Journal* 2016, Volume 16, Issue 7, July/August 2016.

[25] The Court indicated the requirements for any measure to be a lawful interference to privacy rights (requirements deemed, in fact, to be missing in the Data Retention Directive), such as: a) clear and precise rules, i.e., sufficient indications to guarantee the effective protection of personal data retained

Similarly, in the *Schrems* case, the Court found that the adequacy decision did not find that interferences with fundamental rights (although for legitimate purposes) would be limited to those strictly necessary; instead it authorised transfers, subsequent storage and use of data without setting objective criteria to determine related limits, differentiations, exceptions and specific purposes.[26]

2.2.3. *Derogations for law enforcement*

SH principles[27] were not compulsory. As confirmed by the CJEU, the self-certification system is not a problem in itself, as long as adequate guarantees, as well as effective supervision and sanctions mechanisms, exist in the third country for any possible infringements of EU data protection rules. Most importantly, the number of derogations envisaged under the SH principles,[28] such as those for law enforcement and national security purposes,[29] and the way in which these derogations were implemented (i.e. the lack of appropriate limitations), was one of the salient issues in *Schrems*. While derogations for these purposes are in principle legitimate, the Commission's SH adequacy decision lacked any findings that the US application of these derogations would be complemented by sufficient safeguards for EU citizens against the risk of abuse or unlawful access and use of that data. In other words, the adequacy decision did not verify that interference with fundamental rights would be limited to that strictly necessary.[30]

---

against risks of unlawful access or abuse; b) limits on access to data: most importantly, the Retention Directive did not indicate any limits on national authorities' access to the retained data, nor on the use of these data, that is, any limits on the *extent* of the interference with fundamental rights.

[26] *Schrems* judgment, paragraph 93.

[27] See, inter alia, S. Carrera & E. Guild, Safe Harbour or into the storm? EU-US data transfers after the *Schrems* judgment, CEPS publications, 12 November 2015.

[28] See A. Montelero, *'I flussi di dati transfrontalieri e le scelte delle imprese tra SH e Privacy Shield'* in G. Resta - V. Zeno-Zencovich (eds), *La protezione transnazionale dei dati personali. Dai 'SH Principles' al 'Privacy Shield'*, Roma Tre Press, 2016, p. 240, e-book [authors' own translation], who stresses that the rationale behind the SH invalidation lies firstly in its 'anomaly', i.e., in the exceptional nature of political-economic compromise that allowed (notwithstanding the conditions imposed by article 26 of the EU DPD) growing flows of data between EU and US companies. These, however, can no longer be constrained within national borders. In some cases, third countries companies and governments find it more convenient to adopt norms with EU standards (instead of entering into complex negotiations on data transfers). This was not the case with American economic and political powers, and this would explain the reasons for the 'compromise' SH; however, as a consequence of the *Schrems* case, the political machinery on both sides of the Atlantic immediately worked to produce a new (perhaps temporary) agreement, also in view of a reform in the US on data protection and on intelligence power, as urged by both consumers and companies.

[29] The SH established that 'Adherence to these principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; ...'.

[30] See comments by D. Solove, 'Sunken Safe Harbor: 5 Implications of Schrems and US-EU Data Transfer', TechPrivacy, 13 October 2015. In his view, while EU countries also engage in widespread surveillance ('so there is some hypocrisy here'), the US attitude of acceptance of this widespread power of government surveillance without substantial recourse to judicial challenges (i.e. the fact that the NSA could engage in massive surveillance and that people could not challenge that surveillance) is an arrogance of power unacceptable to the EU.

Box 4 – US law enforcement and intelligence and the Schrems case

In *Schrems*, the Court considered that any consideration as regards limitations to the powers of intelligence services and law enforcement agencies (LEAs) to access company data, as well as oversight systems and effective redress mechanisms in case of complaints, was missing from the adequacy decision. As Montelero noted,[31] the original flaw in the Commission adequacy decision was to recognise the adequacy of SH only on the basis of the existence of the agreement (a 'compromise'), without taking into account the broad exemptions envisaged, i.e. that the latter would have prevailed over the obligations on businesses stemming from the SH. Therefore, the Court required the Commission to make an assessment of the implementation of these derogations taking all circumstances into account (DPD, Article 25), particularly the rule of law in force in the USA, and by reasons of its domestic law or of international commitments. Special attention, therefore, has been paid, after *Schrems*, to the status of law and practice in the USA also as regards the power to access to data by law enforcement and intelligence authorities, as well as the redress system.

One of the consequences of the *Schrems* case[32] in the US legal system is precisely the resumption of the discussion on the **Judicial Redress Act (JRA)** in the US Congress.[33] Particular attention has been paid to the adoption of the US JRA, because it allows citizens of countries or regional economic organisations (including the EU), designated by the Department of Justice, to access redress mechanisms in cases of alleged misuse as regards personal data processed under EU-US data transfer agreements. More precisely, it allows 'civil actions under the Privacy Act of 1974 against certain US government agencies for purposes of accessing, amending, or redressing unlawful disclosures of records transferred from a foreign country to the United States to prevent, investigate, detect, or prosecute criminal offenses' (section 2). Notably, EU institutions considered the adoption of the **US Judicial Redress Act** (finally enacted in February 2016) as a prerequisite for the conclusion of the **umbrella agreement**,[34] on data transfers to the USA for law enforcement purposes,[35] which establishes 'for the first time, data protection as the basis for information sharing'.[36]

Moreover, the US Freedom Act 2015 (which modified previous US laws) prohibited bulk collection of telecommunication metadata by intelligence agencies (e.g. NSA) and introduced some transparency requirements. These limitations to bulk metadata collection, together with the restrictions imposed on foreign signals intelligence by **Presidential Policy Directive 28** (2014),[37] are, as discussed below, particularly relevant to the Commission's assessment of the new EU-US data transfer framework. Meanwhile, these legislative measures are considered by several observers and privacy advocates as neither sufficient to solve the surveillance issues nor to provide adequate safeguards.

---

31 A. Montelero, op.cit. footnote 28.

32 At the time of the ruling, only US citizens had access to remedies under the Privacy Act, even if the USA had promised to issue a law enhancing EU citizens' redress rights to protect their privacy. In line with that promise, the Judicial Redress Act was introduced in March 2015 in the House of Representative and in June in the Senate, with the aim of extending the core benefits of the Privacy Act to citizens of major US allies and thereby giving them redress rights under the act. See also K. Archick & M. Weiss, 'US-EU Data Privacy: From Safe Harbor to Privacy Shield', CRS, May 2016.

33 Judicial Redress Act of 2015.

34 See S. Monteleone, EU-US Umbrella Agreement on data protection, EPRS, 2016.

35 In accordance with Art 218 TFEU, the 1 December 2016 the EP gave its consent to the conclusion of the agreement by the Council, which adopted its authorizing decision the day after. The agreement should enter into force during 2017, once the US authorities have completed their internal procedures.

36 EDPS, Preliminary Opinion of 12 February 2016 on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences.

37 Obama Policy Directive no 28/2014, Signals Intelligence activities (section 2).

The European Data Protection Supervisor (EDPS) noted that in *Schrems*, the CJEU interprets Articles 7, 8 and 47 of the CFR in relation to data transfers, all of which apply in commercial as well as in law enforcement areas. Also, when assessing the umbrella agreement, the EDPS took the key findings of *Schrems* into account, and while welcoming the envisaged safeguards, the EDPS recommended improvements for the umbrella agreement to be considered compliant with EU primary law. The improvements would: (a) clarify that all the safeguards apply to all individuals (independently from their nationality); (b) ensure that judicial redress provisions are effective within the meaning of the CFR; (c) clarify that transfers of sensitive data in bulk are not authorised.[38]

In particular, the CJEU stressed that any legislation permitting **access** to individuals' communications by public authorities on a **generalised basis** must be regarded as jeopardising the essence of the fundamental right to the respect of private life; similarly, legislation which does not provide for **legal remedies to individuals** (recourse instruments as regards, e.g., the right to access to their data, the right of rectification, erasure etc.) would not respect the right to effective judicial protection as enshrined in Article 47 of the CFR (§95 of the judgment).

On this point, the **German Schleswig-Holstein** (ULD) DPA was particularly critical in its position paper on the judgment:[39] 'If citizens of the European Union have no effective right to access their personal data or to be heard on the question of surveillance and interception and to enjoy legal protection, article 47 of the CFR is infringed [...] The USA can currently show no effective means to ensure protection essentially equivalent to the level of protection guaranteed within the European Union'.

2.3. The post-*Schrems* transition

The EU and the USA are extremely interconnected markets with trade flow values over US$1 trillion annually and stocks of investment in each economy close to US$4 trillion.[40] In 2012, US exports of up to US$140 billion in value were delivered online to the EU.[41] Cross-data flows can concern different aspect of business life or sectors: the biggest data flows concern human resources data, but can also involve transactions and client information as well as data connected to innovation and R&D, etc.[42] Over

[38] EDPS, Preliminary Opinion.

[39] ULD position paper on the judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14. Moreover, the ULD noted that, if this is the situation in the USA, and given the EU data protection principles, even alternative means such as the data subject's consent cannot be easily invoked as a legal basis, because for consent to be genuine and freely given, it would require that comprehensive information is provided, including about the risks related to the wide derogations in favour of the US authorities: ultimately this would imply that the individual renounce the exercise of their fundamental rights. Some other national DPAs have issued their own positions on the *Schrems* case, such as the Italian Garante, stressing that the ruling requires Member States and EU bodies to ensure real and concrete respect for the CFR.

[40] O. Maisse and G. Sabbati, US: Economic indicators and trade with the EU, EPRS July 2016.

[41] *Ibid*.

[42] These flows can be business to business transactions (B2B), whereby data flows can come from foreign investments and subsidiaries on each side of the Atlantic, or in commercial transactions between firms (R&D data exchange, financial advice, etc.). Data transfer can occur in client to business transactions, as in the case of e-commerce. Global transactions involve transmitting a large amount of personal and sensitive data. The uncertainty created by the invalidity of the SH framework harms both US and EU firms on both sides of the Atlantic. For several examples of potential data transfer across the Atlantic, see: J. P. Meltzer, Examining the EU SH decision and impacts for transatlantic data flows, Brookings Institution, November 2015. Some data on transatlantic digital trade is also available in a study issued by the Policy Department of the European Parliament,

4 000 companies relied on this adequacy decision for their transatlantic data transfers. Small and medium-sized enterprises also rely on SH for cross-data transfers.[43]

By declaring the Commission adequacy decision **invalid**, the CJEU made clear that data transfers to the USA based on the SH principles are no longer in compliance with EU law. As a consequence, companies previously relying on the SH for their transatlantic data flows faced several issues.[44] Some guidance was given by the Article 29 Working Party (Article29WP), the group of EU DPAs, which issued a statement on the implementation of the judgment and on the use of available alternative tools; the Commission did similar in its communication of November 2015.[45]

- The **first issue** concerned the impact on data transfers performed under SH prior to the CJEU ruling. The Article29WP[46] affirmed that transfers still taking place under the SH adequacy decision after the CJEU judgment are unlawful.
- The **second issue** concerned the instruments still available to firms for transferring data (see box below). Here the Article29WP considered existing transfer tools still applicable, such as the binding corporate rules (BCR) or standard contractual clauses (SCC), issued by the Commission under the DPD. A second option could have been to rely on the data subject's unambiguous consent. Under Article 26 of the Data Protection Directive (DPD),[47] in fact, when a third country has not been found to ensure an adequate level of protection (or in the absence of an adequacy decision), transfers can still take place on the basis of alternative grounds, namely the data subject's consent,[48] or if the data controller adduces appropriate safeguards, including by means of contractual clauses. The latter needs to satisfactorily compensate for the absence of a general level of adequate protection.
- The **third issue** concerned the establishment of a transitional period for firms to adjust. The Article29WP gave three months' leeway, stating that coordinated enforcement actions would been taken by the end of January 2016 if no appropriate solution was found with the US authorities.

Box 5 – Binding Corporate Rules and Standard Contractual Clauses

In the absence of a legal framework considered to give adequate data protection guarantees, third country firms willing to use data from the EU can use existing alternative tools, such as the Binding Corporate Rules (BCRs) (an inter-group code of practice, issued by multinational companies) or the Standard Contractual Clauses (SCCs), (issued by the EC under the DPD). The Article29WP considered the use of those tools to allow data flows in the aftermath of the *Schrems* case.

see: P. Chase, S. David-Wilp, T. Ridout, Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies, Directorate General for External Policy – European Parliament.

43 *ibid*.

44 Safe Harbour Data Privacy Briefing: Your Questions Answered by Giovanni Buttarelli, Sidley Austin, 20 October 2015.

45 Statement of the Article 29 Working Party.

46 Article29WP is an independent advisory body on data protection and privacy set up under Article 29 of the Data Protection Directive 95/46/EC.

47 See Article29WP, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (WP 114), adopted on 25 November 2005, which considers the derogations of article 26 to be strictly interpreted.

48 Other alternative bases, relevant in the commercial context, include transfers necessary: for the performance of a contract in response to the subject' request; for the establishment, exercise or defence of legal claims.

Binding Corporate Rules

Firms can decide voluntarily to comply with BCR but, as the name indicates, once adopted those rules become binding on the corporation adopting them. The binding nature of the rules must be clear and sufficient to guarantee compliance outside the European Union/European Economic Area (EU/EEA). This means that a legal entity within the corporation must be responsible under EU law for compliance with the corporate rules and can be subject to enforcement measures in case of non-compliance.[49] Normally, such a responsibility is given to the European headquarters, which must take any necessary measures to guarantee that any foreign member of the corporation aligns their processing activities with the BCR. If the headquarters of the corporate group are not in the EU/EEA, the headquarters must delegate these responsibilities to a member of the corporation based in the EU. Where the group can demonstrate why it is not possible for them to nominate a single entity in the EU/EEA, it can propose other mechanisms of liability that better fit the organisation.[50]

Contractual Clauses and Standard Contractual Clauses

Appropriate contractual clauses (CCs) may also be used to ensure adequate protection safeguards (see article 26(2) of the DPD). These CC must be present in the relation between the controller and the data subject, between the EU/EEA controller and the non-EU/EEA controller, and between the controller and the processor (if the controller outsources the processing to a third country processor not subject to adequate data protection in the third country). These CCs must be assessed by the DPA of the Member State responsible for authorising the transfer. The Member State must inform the Commission and the other Member States of the authorisation granted. The Commission or another Member State may object to the authorisation on justified grounds concerning the protection of privacy and other fundamental rights of individuals.

The Commission may decide, following the comitology procedure referred to under article 31(2) of the DPD, that certain standard contractual clauses (SCCs) provide the appropriate safeguards. The use of these SCCs simplifies the authorisation procedure, as Member States should comply with the Commission decision. The SCCs, as model clauses set up by the EC,[51] lay down obligations for data exporters and importers, including security measures, information for data subjects on transfer of sensitive data, data exporter notification of access requests by third country law enforcement agencies (LEAs), and the right to access, rectify, and erase personal data; these clauses should also state that EU citizens have the possibility to invoke their rights before a DPA or a court in the state of the data exporter. Given the binding force of the Commission Decision, incorporating SCCs in a contract means that national authorities are, in principle, obliged to accept these clauses, i.e. they cannot refuse the transfer of data to a third country. However, in light of the *Schrems* ruling, DPAs retain their power to examine these clauses according to EU law, and in cases of doubt, they may bring a case in front of a national court (which may in turn refer to the CJEU for a preliminary ruling, as per the *Schrems* case). Both data exporters and third country importers subject to a contract containing SCCs, fall under European DPA supervision.

---

[49] In other words, this allows data-subjects to file a complaint to the relevant data protection authority and access redress mechanisms in case of non-compliance with the BCR by the corporation.

[50] One possibility would be to create a joint liability mechanism between the data importers and the data exporters as seen in the EU Standard Contractual Clauses 2001/497/EC (SET I), or to define an alternative liability scheme based on due diligence obligations as prescribed in the EU Standard Contractual Clauses 2004/915/EC (SET II). A final possibility, specifically for transfers made from controllers to processors, is the application of the liability mechanism of the Standard Contractual Clauses 2002/16/EC.

[51] '(EU-)controller to (Non-EU/EEA-)controller': Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, OJ L 181, 4 July 2001, and Commission Decision 2004/915/EC of 27 December 2004, amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29 December 2004; '(EU-)controller to (Non-EU/EEA-)processor' Decision 2010/87/EU (and repealing Decision 2002/16/EC).

2.4. Post-*Schrems* reactions

The CJEU ruling has triggered heated debate in the EU and elsewhere.[52] In this section, we report the main pertinent and authoritative reactions.

In its first statement, in the aftermath of the judgment, the **Article 29 Working Party** (Article29WP) not only clarified the meaning of 'essentially equivalent' in the CJEU's wording as containing 'the substance of the fundamental principles of data protection', but also called for Member States and European institutions to urgently find a solution to overcome the situation of uncertainty, including obligations on oversight mechanisms, transparency, proportionality, and redress means with the US authorities.[53]

In line with the position of the Article29WP, some of the **national Data Protection Authorities** (DPAs) have not only forbidden transfers in their countries on the basis of the current SH regime, but have reaffirmed their power to carry out controls on the lawfulness of data transfers by data exporters.[54] Joint guidance by the **16 German DPAs** followed, in which it was made clear that: 1) transfers based solely on the SH were prohibited, as SH has been invalidated; 2) apparently in discontinuity with the other DPAs, the German DPAs temporarily suspended new approvals of BCRs and data export agreements, and put the validity of data transfers based on EU model clauses into question.[55]

A number of **EU-US NGOs** (such as EPIC and Privacy International) wrote a joint 'Letter on the Safe Harbour after *Schrems*', addressed to both Commissioner Jourová and US Secretary of Commerce Pritzker, in which they affirmed that 'a revised SH framework similar to the earlier SH will almost certainly be found invalid by the CJEU' and claimed that the *Schrems* ruling required 'necessary changes in the domestic law and international commitments of the negotiators ...'.[56] In particular, they pointed to the CJEU emphasis on the requirement that a third country should ensure effective protection, as well as to the halting of mass collection of e-communication contents, and on the admissibility of limitations to data protection only when strictly necessary.

---

[52] See examples in European and US news. See also the statement by US Secretary of Commerce Penny Pritzker on European Court of Justice SH Framework Decision, of 6 October 2015.

[53] Article 29 Working Party Statement of 16 October 2016.

[54] Among the first reactions to the *Schrems* ruling, **the German DPA of Schleswig-Holstein** issued a position paper on 14 October 2015. As for other DPAs, the Italian **Garante** ruled that current transfers based on its previous authorisation were forbidden, while companies were allowed to use other tools (i.e., SCC and BCR, as well as specific Garante authorisations). The Spanish DPA (**AEPD**), required companies operating in Spain to make sure that alternative mechanisms were implemented for data transferred to the USA, warning them of possible enforcement actions if they failed to adopt and notify these mechanisms to the same AEPD. A similar position was taken by the French CNIL.

[55] The German DPAs reaffirmed their power to prohibit transfers based on EU model clauses, and indeed they exercised this power, after deciding that a specific data transfer was invalid.

[56] See the joint letter, p. 8: 'the EU should end the mass surveillance of people by Member States'; 'the EU should suspend the Swift Agreement and the PNR Agreement and pursue a digital bill of rights as recommended by the European Parliament Civil Liberties, Justice & Home Affairs (LIBE) Committee (electronic mass surveillance of EU citizens report)'; 'the US should enact a comprehensive legal framework on data protection based on the Consumer Privacy Bill of Rights with appropriate regulatory and enforcement powers'; 'the USA should establish an independent data protection agency'; 'the USA should ratify Council of Europe Convention 108'.

Some **US technology companies** saw the striking down of the SH as a wake-up call for businesses, which may expect a regulatory domino effect to occur region by region, and urged companies to be proactive in complying with the new regulations.[57]

The **European Parliament** holds a long-standing position regarding the lack of adequate level of protection of fundamental rights under the SH regime and, in addition to conducting several enquires, has repeatedly called for the suspension of SH principles, in particular in its 2014 resolution on the electronic mass surveillance programmes run in the USA and in some EU countries.[58] In the aftermath of the CJEU ruling, the case and its consequences were debated in the EP.[59] On 29 October 2015, a follow-up to the 2014 resolution was adopted,[60] in which the EP also stressed the significance of the other CJEU ruling[61] declaring the Data Retention Directive invalid. The novel aspect of *Schrems* is also represented by the reference made by the CJEU to the principles expressed by the European Court of Human Rights (**ECtHR**) in its case law concerning the issue of limits to 'general programmes of surveillance'.[62] The reciprocal reference between the two courts on data protection matters (and its timing) is particularly meaningful.[63]

In its 2015 follow-up resolution, the EP also considered reforms conducted in the USA on surveillance legislation were significant for the development and implementation of the new framework, in particular the adoption of the US Judicial Redress Act.[64] Regarding democratic oversight, the EP mentioned that: 'While fully respecting that national

---

57 Ron Hovsepian, Living In A Post-Safe Harbor World, CloudTweaks, 30 November 2016.

58 EP, Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights.

59 LIBE Chair, Claude Moraes (S&D, United Kingdom), urged the Commission to initiate a new data transfer framework, affirming: 'It is commercial, it is business, it is citizen's freedoms, but it is also a day to day matter'.

60 EP, Resolution of 29 October 2015 on the follow-up to European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens.

61 See footnote 23.

62 On the mutual references in the ECtHR and CJEU case law see F. Bohem, 'Assessing the New Instruments in EU-US Data Protection Law', EDPL 2/2016, who also stresses the increasing interconnection between law enforcement and pure surveillance contexts in the USA and EU (with data exchanged between agencies of different sectors), that seems reflected in the lack of distinction made by each court when referring to the other court's arguments. See also Fundamental Rights Agency report, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU', 2015. The CJEU is therefore expected to also apply the same reasoning of the ECtHR in future when assessing the validity, under the CFR of Fundamental Rights (CFR), of other EU and Member State legislative acts in this same field.

63 See P. de Hert & P. C. Bocos, 'the Case of *Roman Zakharov* v. *Russia*: The Strasbourg follow-up to the Luxembourg Court's *Schrems* judgment, Strasbourg Observers, 2016.

64 In its 2015 follow-up Resolution, the EP '[...]welcomes the fact that the Judicial Redress Act of 2015 was successfully passed by the House of Representatives on 20 October 2015, underlining the substantial and positive steps taken by the USA to meet EU concerns; considers it of paramount importance to ensure the same rights in all the same circumstances of effective judicial redress for EU citizens/individuals [...]'; the EP underlines that one prerequisite for signature and conclusion of the umbrella agreement is the adoption of the Judicial Redress Act in the US Congress; [...] and, with regard to the umbrella agreement: '[...] Recalls that any international agreement concluded by the EU takes precedence over EU secondary law, and therefore stresses the need to ensure that the umbrella agreement does not restrict the data subject rights and safeguards applying to data transfer in accordance with EU law'.

parliaments have full competence in the oversight of national intelligence services, calls on all those national parliaments which have not yet done so to thoroughly evaluate and install meaningful oversight of intelligence activities and to ensure that such oversight committees/bodies [are] able to effectively and independently oversee intelligence services and information exchanges with other foreign intelligence services.'[65]

3. Privacy Shield: a long path

3.1. First Commission adequacy decision and new 'privacy principles'

The new adequacy decision on the 'Privacy Shield' (PS) adopted by the European Commission on 12 July 2016 as the new framework needs to comply with CJEU indications (*Schrems* and other cases). The different steps in the procedure that brought the new framework to adoption deserve consideration.

The Commission and the US Department of Commerce have been reviewing the SH framework for at least the last two years, and after *Schrems* negotiations on this work intensified in order to reach a new agreement. A substantial part of the negotiations were represented by an intense exchange of information between both sides of the Atlantic on how the US data protection system works and by commitments on stronger safeguards in order for the Commission to make a clear assessment of the US system in view of the adoption of a new adequacy decision.[66]

To this aim, the Commissioner for Justice, Consumers and Gender Equality, **Vera Jourová**, announced that a **new political deal**, the **Privacy Shield** (PS), had been reached with the USA, at an EP Civil Liberties, Justice & Home Affairs (LIBE) Committee meeting on 2 February 2016 (although no text was made available at that time). On that occasion, Commissioner Jourová, stressed that 'the USA has given written assurance that the possibility for national security and law enforcement authorities to access personal data will be subject to clear limitations, safeguards and oversight mechanisms and ... will not engage in indiscriminate mass surveillance', suggesting that the ongoing reform of redress mechanisms and data protection was under the spotlight in the USA.[67]

In addition, on 2 February 2016, the European **Article 29 Working Party** released a first statement on the Privacy Shield announcement, in which it pointed out **four main guarantees** for intelligence activities on which it would have based its assessment (once the documents on the Privacy Shield were made public) and that are inferred from the European jurisprudence on fundamental rights:

(1) data processing should be based on clear, precise and accessible rules: anyone should be able to envisage what will happen to their data and where they are going to be transferred;

---

[65] *Ibid*. paragraph 20.

[66] As a recent study commissioned by the LIBE Committee clarifies, there is, so far, a huge difference between the USA and EU data protection systems, at the constitutional, procedural and redress level. Therefore, future data transfers seem to be strongly linked to ongoing reform of the US legislation, in particular on surveillance and law enforcement activities. See the study by Franziska Boehm, 'A comparison between US and EU data protection legislation for law enforcement purposes', commissioned by EP Policy Department C for the LIBE Committee.

[67] Commissioner Jourová's announcement of the new agreement.

(2) proved necessity and proportionality with regard to the legitimate objectives pursued (national security);
(3) an independent, effective and impartial oversight mechanism (either a judge or another independent body);
(4) effective remedies available to anyone.

While the Article29WP recognised US efforts in 2014 and 2015 to improve data protection for non-US citizens, in this statement it confirmed its concerns about the current US legal framework as regards the four essential guarantees, especially regarding scope and remedies. The Article29WP also recalled that, given the invalidation of the SH, EU DPAs were dealing with related cases and complaints on a case-by-case basis.[68]

On 29 February 2016, the Commission released a package of documents, constituting the **first version of the new EU-US Privacy Shield framework** and including:

- a **communication** from the European Commission to the EP and the Council: 'transatlantic data flows: restoring trust through strong safeguards;
- the European Commission **draft adequacy decision**;
- the '**privacy principles**' as released by the US Department of Commerce (DoC);
- **several letters** containing 'commitments' from the US authorities, both from the commercial as well as the intelligence and law enforcement sectors; also including letters from State Secretary John Kerry and the presidents of both the DoC and Federal Trade Commission (FTC) (Annexes).[69]

3.2. Opinion, analysis and reactions to the first version of the Privacy Shield

As seen in the hearing organised by the EP LIBE Committee[70] and in the media,[71] reactions to the publication of the (draft) PS were lukewarm (if not critical),[72] in particular pointing to the fact that it still allows US intelligence to collect massive and indiscriminate data and use them at least in six specific cases,[73] and that new challenges could be brought to the court.

As part of the procedure for the adoption of the Commission adequacy decision (Article 25 DPD), the Article29WP, the Group of European DPAs, provided an opinion on the draft new framework before its adoption. Additionally, the DPD prescribes that representatives of Member States, grouped in the **article 31 Committee**, approve the

---

[68] Statement of the Article 29 Working Party on the consequences of the *Schrems* judgment. See also press conference of 3 February 2016, held by the chair, Isabelle Falque-Pierrotin.

[69] See European Commission press release of 29 February 2016.

[70] EP, hearing of 3 March 2016, *The new EU-US Privacy Shield for commercial transfers of EU personal data to the US*.

[71] Among others: Glyn Moody, 'Privacy Shield' proposed to replace US-EU Safe Harbor, faces skepticism, Ars technica, 29 February 2016.

[72] See inter alia, G. Vermeulen, 2016. 'The Paper Shield: On the Degree of Protection of the EU-US Privacy Shield Against Unnecessary or Disproportionate Data Collection by the US Intelligence and Law Enforcement Services' in D. Svantesson and D. Kloza (eds), *Transatlantic Data Privacy Relationships as a Challenge for Democracy*, Intersentia, 2016.

[73] As the Obama Policy Directive no 28/2014, Signals Intelligence activities, recalled in the Privacy Shield adequacy decision, indicates.

decision.[74] The expected Article29WP **assessment** of the new deal was released on 13 April 2016.[75] In this opinion, the Article29WP welcomed the efforts made on both sides of the Atlantic to achieve a new framework for data transfers and recognised improvements compared to its predecessor (SH). However, it expressed concerns about some aspects that they asked the Commission to address and to clarify. Moreover, the opinion contained recommendations for improving the (draft) adequacy decision. In particular, the opinion critically assessed both the commercial aspects (part I) and US public authority access to data transferred under the PS (part II). The **lack of clarity** in some parts of the Commission's adequacy decision, the **doubtful independence of the proposed US Ombudsman**, the remaining **possibility of bulk collection of data** and the **complex systems of redress mechanisms** were the main points of **criticism**.

With regard to the commercial aspects, the Article29WP asked for more clarity, and ameliorations with regard to data retention and purpose limitation principles, as well as to automated individual decisions and onward transfers.

In the second part, on US public authority access to data transferred under the PS,[76] the main criticisms focus on the lack of concrete elements regarding the proportionality of data collection, as 'tailored data processing can still be considered to be massive': concerns in this regard remain, despite the limitations introduced by legislation after 2013.[77] Moreover, as regards the judicial remedies, the Article29WP notes that the US system has an important limit, requiring the individual to demonstrate their standing, i.e., the applicant needs to sustain direct injury or harm. This approach is different from the European stance, where anyone can go to court if they have a legitimate reason to suspect interference with their fundamental rights.[78] In addition, the US requirement appears thwarted by the lack of notification to individuals subject to surveillance measures even after they have ended.

While the opinion was not binding, the Commission was invited to follow the indications for improvements. It is worth noting that the European authorities will play a role in ensuring that the PS is implemented, as they will have the power to receive/investigate complaints about the agreement.

The European Data Protection Supervisor (**EDPS**), commenting on the Article29WP opinion,[79] clarified that, while the Privacy Shield (PS) can be considered a development

---

74 See the comitology procedure and documents.

75 Article 29 WP Opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision, 13 April 2016.

76 This part of the opinion is complemented by another document in which the DP authorities have confirmed **four essential guarantees** for justifiable security measures that constitute an interference with fundamental rights (data processing in accordance with the law and based on precise and accessible rules; necessity and proportionality with regard to the legitimate objectives pursued to be demonstrated; existence of an independent oversight mechanism; effective remedies available to the individual).These guarantees have to be respected in any case of data transfer to third countries.

77 The Article29WP could not make, in its Opinion, a final assessment as to the legality of targeted but still massive processing of data, not least because it was awaiting the CJEU's position. Limitations at least to general and indiscriminate data *retention* have in fact been recently reaffirmed by the CJEU in Joined Cases C-203/15 and C-698/15 - *Watson & others* along with *Tele2Sverige*; see also the pending case on EU-Canada PNR)..

78 As clarified by the ECtHR in *Zakharov*, and quoted in the Article29WP opinion.

79 See Giovanni Buttarelli, presenting the EDPS Annual Report 2015 to the EP LIBE Committee.

compared to Safe Harbour (SH), the measure by which it should be assessed remains the DPD, therefore robust improvements to the draft text of the PS were needed. In addition, the EDPS stressed that, while binding corporate rules (BCR) or standard contractual clauses (SCCs) may work well for big companies (to cover their data transfer), many small and medium-sized enterprises (SMEs) or small companies need a new solution, which should also be considered in view of the new General Data Protection Regulation (**GDPR**), so that companies are not requested to change their privacy polices again once the new Regulation is applied. The EDPS called, in other words, for **future-oriented thinking**. Besides taking part in the work of the Article29WP, the EDPS has also released an assessment and recommendations. In the EDPS **opinion** of 30 May 2016, the Supervisor urged for robust improvements to achieve a solid and sustainable framework (a long term solution). In particular, while welcoming the efforts made by both parties to find a solution for data transfers (crucial in an era of 'global, instantaneous, unpredictable data flows') and appreciating the increased US transparency with regard to intelligence practices aimed at collecting non-US citizen data, the EDPS stressed that the new framework needs to reflect shared democratic and individual rights-based values.[80]

After some delay, on 8 July 2016, representatives of **European Member States** (article 31 committee) voted (with four abstentions) for the adoption of the PS package.[81]

The **European Parliament** (EP), which has no voting power in Commission implementing decisions, voiced its concerns regarding the new framework by adopting a (non-binding) **Resolution** on 26 May 2016,[82] in which it called upon the Commission to 'implement fully the recommendations expressed by the Article29WP, in order to reach a robust Privacy Shield'. Among the relevant points of the Resolution, on the one hand, the EP underlined the meaning of protecting data as 'protecting the people' to whom the information being processed relates, as data protection is one of the fundamental rights recognised in the CFR, and on the other, it stressed the relevance of legal certainty in data transfers for

[80] EDPS Opinion 4/2016. Accordingly, the draft PS could be considered as a step in the right direction, but did not include (as formulated at that time) all appropriate safeguards to protect individual rights as required by the Treaty and the CFR. See also X. Tracol, EU-US PS: the saga continues, Computer Law & Security Review 32 (2016), 775-777, claiming that the European Commission again failed to provide an overall assessment of the US legal order and relied only on letters from various authorities.

[81] See the formal vote of the article 31 Committee. In case of a negative vote by the article 31 Committee, the Commission could have appealed or submitted a revised version of its adequacy decision. Commissioners Jourová and Ansip announced the endorsement in a joint statement on the same day, declaring that 'For the first time, the US has given the EU written assurance that the public authority access for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms and has ruled out indiscriminate mass surveillance of European citizens' data [...] and protects fundamental rights and provides for several accessible and affordable redress mechanisms'.

[82] EP, Resolution on transatlantic data flows, 26 May 2016. While this highlights the importance of the transatlantic relationship, the Resolution underlined that 'PS should be in compliance with EU primary and secondary law as well as with the relevant rulings of both the **CJEU** and the **ECHR**'. During the debate on the EP Resolution, several amendments (seven) proposed by different political groups were rejected. Many MEPs questioned whether the PS would stand up in court, and the left wing MEPs led by Jan Philipp Albrecht (Greens, Germany), proposed to include a 'sunset clause' as a minimum requirement in the Privacy Shield – a time frame of four years, after which a review of the deal would be necessary, in view of the new US administration and the implementation of the GDPR.

consumer trust, transatlantic business[83] and law enforcement cooperation. Moreover, the EP stressed that 'the Privacy Shield is part of a broader dialogue between the EU and third countries ... in relation to data privacy ... and objectives of shared interest', underlining the need to define a general approach on data transfers to third countries.[84]

In her statement to the EP, **Commissioner Jourová** recognised that the PS may be not perfect, but that the Commission was satisfied with having achieved the maximum possible.[85]

However, criticisms were made on the draft PS. **Human Rights advocates** and other observers considered the US 'commitments' too vague and weak[86] to guarantee the respect of EU citizens' rights and envisaged that the PS would meet the same fate as the SH.[87] At the same time, some publications have highlighted criticisms of the CJEU ruling.[88]

4. Revised Privacy Shield

Concerns expressed in the EU prompted modifications to the draft adequacy decision. The new, amended decision, establishing that the new EU-US framework provides for

---

[83] In particular, the Resolution recalled (recital E) the fact that prompt achievement of a new deal was particularly needed for SMEs, which account for 60% of the companies relying on the former SH, i.e. of companies allowed to benefit from streamlined and reduced compliance procedures.

[84] For instance to China, as has been discussed by the EP.

[85] Debates took place on 25-26 May 2016 in the EP. The EU Commissioner for the Digital Single Market, Andrus Ansip, pronounced confidence that the new deal would allow EU citizens several mechanisms for resolving disputes with companies. On the necessity to achieve a transatlantic agreement (of any degree) to protect the citizens on both sides of the Atlantic against surveillance by US and European intelligence agencies (as US citizens would also be vulnerable to surveillance by European states), see D. Cole and F. Fabbrini, 'Bridging the transatlantic divide?: The United States, the European Union, and the protection of privacy across borders', International Journal of Constitutional Law (2016) 14 (1).

[86] See, inter alia: Anna Fielder, 'From an unSafe Harbour to a Privacy Shield full of holes', Privacy International, 12 April 2016; Allison Deighton, 'The EU-US Privacy Shield – is it strong enough?' PDPRO Privacy & Data Protection, 2016, 16 (4), 8-10; TLT solicitors, who noted at least two main threats likely to challenge these commitments: the Presidential Policy Directive (that currently binds US intelligence authorities, restricting the extent of surveillance activities) might well be replaced by the next US administration; secondly, in any case of concern about the binding nature of these commitments, the new agreement on transatlantic data transfer may be challenged in the same way as the SH. On the nature of the US commitments, the Commission, during a January debate in Parliament's LIBE Committee on the draft motion for a resolution on Privacy Shield, has pointed out that, independently from the change in the US administration, the continuously existing commitments are binding for the USA (not for this or that administration).

[87] Ars Technica reported the fears of many that the NSA will continue to have broad powers in certain cases, regardless of the concerns voiced by privacy advocates. Privacy activist Max Schrems claimed that faced with 'the existence of an explicit US law allowing mass surveillance [...] the US openly confirms that it violates EU fundamental rights in at least six cases.'

[88] David Bender, 'Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective', International Data Privacy law, 2016, Vol 6, No 2; Lothar Determann, 'Adequacy of data protection in the USA: myths and facts', International Data Privacy Law, 2016, Vol 6, No 3, who claims that: 'If better data protection levels is the true objective of updating the Safe Harbour programme, then the EU should consider making the reach of the programme bidirectional and also apply and enforce the more effective, specific and up-to-date US data privacy laws in Europe'. On the importance of a transatlantic deal see also J. Brill 'Strengthening International Ties Can Support Increased Convergence of Privacy Regimes', European Data Protection Law Review, Vol 2 (2016), Issue 2.

adequate protection for European citizens' data, was **finally adopted** on **12 July 2016**, by the Commission, in college, so that the new PS on data transfers was 'running before summer 2016 ... to put an end to the current legal uncertainty'.[89] The adequacy decision was notified to the Member States the same day, and thereby entered into force immediately. On the US side, the Privacy Shield framework was published in the **Federal Register**, the equivalent of the European Union Official Journal, although a further couple of weeks was allowed for companies to 'transit' to the new regime. The new regime is now fully operational.

Among the changes promised, and in line with articles 25 & 26 of the Data Protection Directive as interpreted by the CJEU in *Schrems*, it was established that the adequacy of the level of data protection should be assessed regularly, considering the whole situation and legal practices: the new deal therefore also provides for an **annual joint review** of the PS.

Beginning from 1 August 2016,US-based companies (which, as noted previously, relied on more complex data transfer schemes like BCR in the transitional period), could sign up to the Privacy Shield. That is, they began to **self-certify** their compliance with the new framework with the DoC. The DoC has to verify that their privacy policies comply with the high data protection standards required by the PS. In practice, they are encouraged to publicly commit to comply with the framework's requirements by registering via an ad hoc **website**,[90] which explains:

> 'The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables U.S.-based organizations to join the Privacy Shield Framework in order to benefit from the adequacy determination [of EC] ... While joining the Privacy Shield Framework is voluntary, once an eligible organization makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under U.S. law. All organizations interested in joining the Privacy Shield Framework should review its requirements in their entirety.'

In parallel, the Commission released a **guide to the EU-US Privacy Shield**,[91] to which the Article 29 Working Party committed to comment in the following months. The guide,

---

89 As requested by Commissioner Jourová at the LIBE Committee meeting held on 11 July 2016, where she provided the state of play on the PS.

90 Privacy Shield Framework.

91 The guide first stresses how data transfers to the US are necessary to the transatlantic relationship (especially in today's global digital economy) and why PS is needed to ensure that data transferred to the US continue to benefit from a high level of protection. Worthy of note is that it clarifies that the protection applies regardless of whether the data subject is an EU citizen or not (as requested by the Article29WP, to make sure that the right is recognised for any individual, according to the CFR, independently of their respective nationality). However, it remains to be clarified whether judicial remedies under the JRA are also available to EU residents or only to EU citizens. The guide also explains that PS is one of the possible tools available (besides contractual clauses and BCR), but if companies sign up to the PS framework, they must have a privacy policy in line with the 'privacy principles', where the obligations for companies under the PS are indicated; a list of companies taking part in the PS (as well as those no longer taking part) is made available on the DoC website. The DoC should ensure 'that companies live up to their commitments' (companies can only keep data if they 'commit' to the DoC that they will continue to apply the privacy principles). If companies do not review their 'membership to the PS annually, they can no longer receive and use data from the US under the PS framework (i.e., they can continue on the basis of other tools).

which is mainly addressed at individuals, is a brief and informative publication meant to clarify some of the issues at stake: it contains indications of the PS company obligations, on individual rights and redress mechanisms; the publication explains how to make a complaint against a company (through several avenues) or against a US public authority (e.g., via the new Ombudsperson).

4.1. Privacy principles and firms' obligations

While the principles appear similar to the SH principles at first sight, the new PS developed them to include a number of changes in obligations on companies that these principles entail.

The first principle of '**notice**' required in the SH that organisations have to notify individuals about the purposes for which they collect and use information about them; as well as on how individuals could contact the organisation with any inquiries or complaints; on the types of third parties to which they disclosed the information and the choices and means the organisation offers for limiting the data's use and disclosure. While this principle is maintained in the PS, it also includes an obligation to make their privacy policies public (indicating that they conform to the PS principles),[92] and has to provide links to these and further information to the DoC. Moreover the principle now includes designation of an independent dispute resolution body designed to address complaints. Originally, the principle of notice was not applicable to transfer to a third party which acted as agent under instruction of the company. This latter situation was covered only by the principle on onward transfer. This exception was changed in the new PS, so that the companies must now provide data subjects with information regarding right of access and choice as well as regarding onward transfers.

The second principle of **choice** under the SH required organisations to give individuals the opportunity to choose (opt out) whether their personal information would be **disclosed to a third party** (controller) or used for a **different purpose** (even if incompatible) than the original purpose of data collection. For sensitive information, affirmative or explicit choice (opt in) had to be given if the information was to be disclosed to a third party or used for a different purpose. Currently, the PS allows opt outs where a new, changed, purpose is **materially different but still compatible with the original purpose** (as recommended by the Article29WP). The PS expressly states that the **choice principle cannot be used to supersede the prohibition on incompatible processing**. This is a fundamental change from the SH. However, the PS remains unclear about the timing for data subjects to avail themselves of their opt out right; the PS clearly gives data subjects the right to object at any time for direct marketing purposes only,[93] while remaining silent on other cases of opt out.[94]

The third principle on **onward transfers** (transfers to third parties) deals with disclosure of data to a third party. In SH, organisations had to apply the notice and choice principles. These principles were waived in the SH for organisations who wished to transfer data to a third party acting as an agent of the company in three circumstances: (1) ensuring that

---

92 See also supplemental principle 'verification', annex II, III, 7 of the Privacy Shield.

93 See annex II of the Implementing Decision on EU-US Privacy Shield Framework Principles issued by the US Department of Commerce, pp. 20 and 42.

94 In this regard, the **Article29WP** regretted the lack of a general right to object, i.e. whenever the individual has compelling legitimate grounds relating to his particular situation.

the third party subscribed to the SH privacy principles; or (2) the third party was subject to the DPD or another adequacy finding; or (3) the SH organisation had entered into a written agreement with such a third party requiring it to provide at least the same level of privacy protection as required in the SH. In the PS, the notice principle is always applicable, even as regards onward transfer, while the derogation for onward transfer to third parties acting as agents (processors) remains applicable to the choice principle, i.e. individuals will have no opt out right in this case.[95] Nevertheless, the organisation has an obligation to enter into a contract with the agent. As requested by the Article29WP, the final adequacy decision on the Privacy Shield was amended to stress how the onward transfer should ensure equivalent level of protection as guaranteed by the principles of the PS.[96] This requirement implies inter alia that the third party must process the data only for purposes not incompatible with the original purpose for which the data was collected and the data subject had authorised. This requirement applies to **all third party transfers irrespective of their location**.[97] To comply with this requirement, the organisation has to: conclude a contract with the third party specifying that, if the third party can no longer comply with the PS principles, notification must be made to the original organisation and processing of the data transferred by third party must be halted; any other steps necessary must be taken to remedy the situation. Moreover, if compliance issues arise in the context of sub-processing of the data, the original organisation acting as a controller will be held responsible, unless it can prove that it was not responsible for the damage or otherwise face liability.

Access to personal information held by an organisation had to be given to data subject under the SH principles. Data subjects could ask to correct, amend, or delete that information where the latter was inaccurate. However, access could have been denied where the burden or expense of providing access would have been disproportionate to the risks to the individual's privacy, or where the rights of persons other than the individual could have been violated. **The PS transforms this principle into a fully-fledged right of data subjects**. Data subjects can obtain confirmation that their personal data are processed by an organisation, without the need for justification, and only against a non-excessive fee, and must receive the data requested in a reasonable time. The PS further regulates **the exception** to access to data by stating the following conditions: (1) existence of an exceptional circumstance; (2) the limitation to access is necessary and duly justified; (3) the burden of proof rests on the organisation to prove that such requirements are fulfilled.[98] On the question of **automated decision-making** based on

---

[95] See annex II of the Implementing Decision on EU-US Privacy Shield Framework Principles issued by the US Department of Commerce, p. 20.

[96] See the Article29WP April 2016 opinion, p. 20, Commission adequacy decision p. 8 and annex II.II.3.

[97] Article29WP in its April 2016 opinion (p. 22) welcomed the 'accountability for onward transfers' principle, allowing transfers to agents (processors), on the base of a contract, only for limited and specific purposes, but also asked that these limited purposes should be compatible with the initial purposes. The new text of PS now includes a requirement to be 'consistent with the consent provided by the individual'. Moreover, the text asked additional obligations and clarification as regards the transfer to a subsequent processor (agent), as the original EU controller should not be deprived of their control capacities and has to be informed of other onward transfers: the contract between the EU controller and the first agent determines whether an onward transfer is allowed (p. 23).

[98] To note that the Article29WP asked for clarification that the limitation contained in supplemental principle 8 (access needs to be provided only to the extent that an organisation stores the data) should

automated processing,[99] the adopted implementing decision on the PS, as opposed to the first draft, contains a reference to specific US law regarding protection of the individual in areas where automated processing is used (credit lending, mortgage offers).[100] It further suggests the need to discuss profiling, which is covered in the GDPR; exchanges on this issue will form part of the first annual review.

The PS **reinforces the security requirement**. In the SH, this principle only required organisations to take reasonable precautions to protect personal information from loss, misuse, and unauthorised access, disclosure, alteration and destruction. The Privacy Shield requires reasonable and appropriate security measures to be put in place. These measures must be assessed by taking into account the risks involved in the processing and the nature of the data. Moreover the PS requires a contract is concluded with any sub-contractors, guaranteeing the same level of protection.

Under the SH, the sixth principle, **data integrity** of personal information required data collected to be relevant for the purposes for which it was intended, and that the organisation ensure that data was reliable, accurate, complete, and current. This principle was amended in the PS to also include the **purpose limitation principle**. This principle states that organisations cannot process data for purposes incompatible to those for which data is collected from and authorised by the data subject. It also now specifies that data can only be retained as long as it serves to fulfil the purpose for which the data was collected and processing authorised. Data can be retained for longer periods, subject to the PS safeguards, only for the time and to the extent such processing reasonably serves one of the following purposes: archiving in the public interest, journalism,[101] literature and art, scientific and historical research, and statistical analysis. There seems therefore to be no explicit obligation on the firm to define a specific time limit for its data retention in their privacy policy; the firms are instead obliged to mention the purpose for which the data is collected.

The last principle from the SH included **enforcement obligations**, and was complemented in the PS. Analysis of these is developed in the next section.

4.2. New redress mechanisms

The Safe Harbour introduced **enforcement obligations** to ensure organisations comply with the SH principles. Organisations had to make independent recourse mechanisms to investigate individual's complaints readily available and affordable, and award damages

be interpreted restrictively, equalising 'storing' with 'processing' in any way. This latter suggestion has not been taken up.

[99] Automated means such as computers may use algorithm and other rule-based systems to take decisions automatically on and for the individuals on the basis of personal information stored in the data. In the EU Data Protection Directive (article 15), individuals have the right not to be subject to decisions taken on the basis of automated processing.

[100] See adequacy decision p. 7. However, see also the Article29WP opinion, which criticised the number of exceptions provided under the supplemental principle, access (annex II, III, 8.e. (i), confirmed in the adopted PS, and its latest statement, in which it regrets the lack of specific rules in Privacy Shield on automated decisions. On enforcement issues in data protection in general see D. Wright & P. De Hert (eds), Enforcing Privacy: Regulatory, Legal and Technological Approaches, Springer, 2016.

[101] The Article29WP would have preferred a more limited approach to journalistic exemptions to the processing and retention of data as provided by the PS, in line with the CJEU view (e.g. *Google Spain* case).

where applicable. Firms had also to ensure that procedures for verifying implementation of the SH principles were in place, and that they remedied any problems arising from the failure to comply with the SH principles. Sanctions had to be sufficiently rigorous to ensure compliance by the organisation. Finally redress mechanisms could be found via section 5 of the Federal Trade Commission (FTC) Act. However, cooperation with Data Protection Authorities (DPAs) was facultative.

The Privacy Shield (PS) develops the redress avenues. In particular it makes cooperation with DPAs obligatory for participating organisations that process **human resources data**. For other organisations, cooperation with DPAs remain facultative; organisations can choose the DPA as their independent resolution mechanism instead of other alternative dispute settlement mechanisms. Moreover, the PS introduces **recourse mechanisms in case of non-compliance** with a ruling from the dispute resolution or self-regulatory bodies. In this case, the dispute resolution or self-regulatory body must notify cases of non-compliance with rulings to the DoC and the FTC (or other US authorities with jurisdiction to investigate unfair and deceptive practices), or a competent court. As a last resort, parties may bring the claim before a **Privacy Shield panel**.[102]

The Commission envisages different possible steps of recourse.

(1) Data subjects may send a complaint directly to the self-certified company. The company must have established an effective redress mechanism and must inform individuals of a contact point to which claims can be sent. The contact point can be internal or external to the company. Claims may also be sent by the data subject via the DoC or the DPA. The firm must answer the claim within 45 days.

(2) Claims can be brought in front of the independent dispute resolution body designated by the organisation to resolve the individual complaints, free of charge. Such a dispute resolution body must provide a decision that may include sanctions and remedies, as well as an end to the non-compliant situation. The independent dispute resolutions body must provide information regarding the PS and the procedures. They must also provide annual statistics on the services they provided. In case the company does not comply with the ruling of a dispute resolution body, then the data subject can still bring claims before the FTC or any other US authority who has jurisdiction to investigate unfair and deceptive practices in the US.

(3) The data subject can seek redress before the DPA if the company is obliged or accepts to cooperate. Obligation to cooperate with the DPA is only imposed on PS companies that process EU individuals' human resources data; other companies may accept cooperation voluntarily. The DPA delivers its opinion via an informal panel of DPAs established at EU level. Both sides are given the opportunity to comment on the claim before advice is issued by the panel. Companies who are subject to cooperation with DPAs are obliged to answer to enquiries and must comply with the advice given by the DPAs' panel, including with any remedial and compensatory measures required. Advice by the panel must be issued within 60 days of receiving the complaint and the organisation has 25 days after the delivery of the advice to comply.

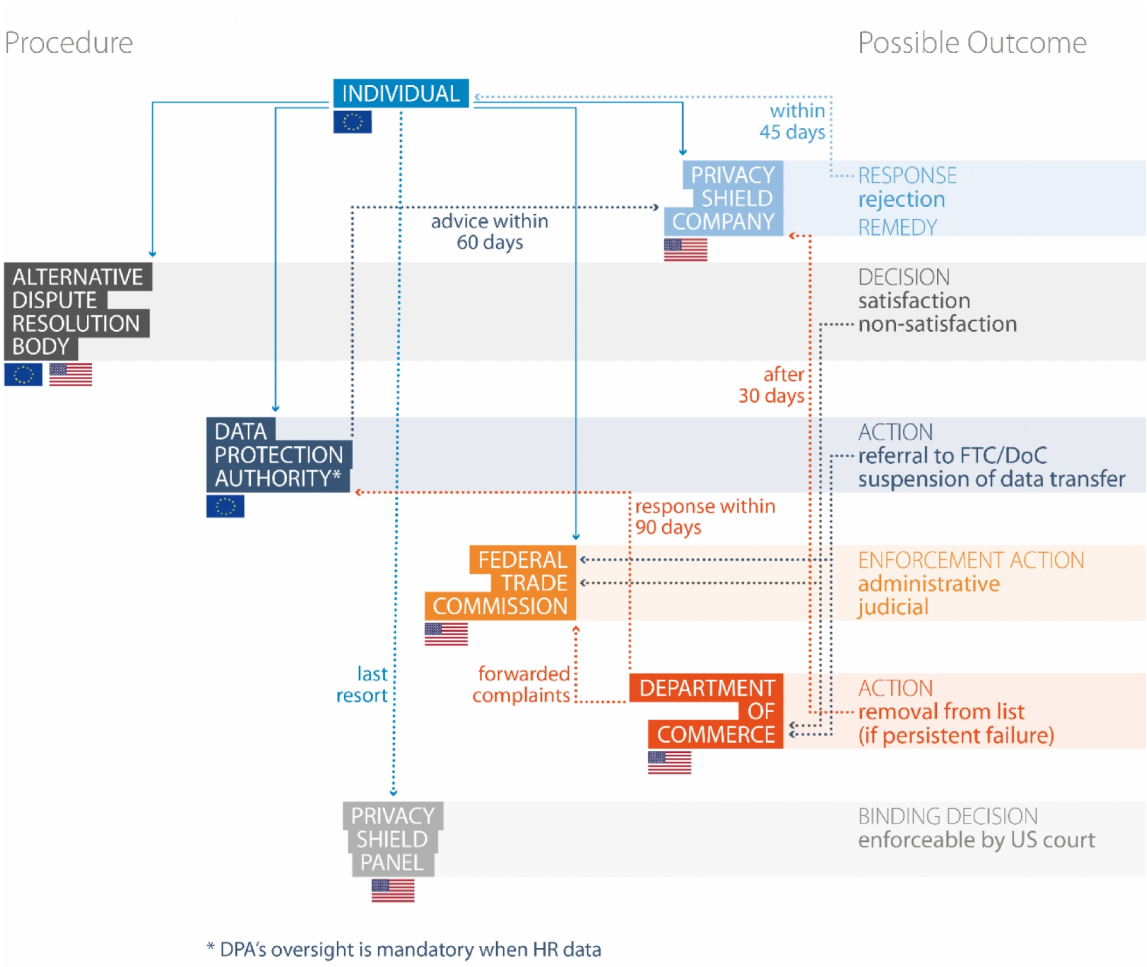
(4) In case of unjustified non-compliance with the advice of the panel of DPAs, the latter can give notice of either submitting the claim to the jurisdiction of the FTC, or concluding that there was a breach of the cooperation requirement. In the first case, this may lead to enforcement action based on section 5 of the FTC Act (as explained

[102] The Article29WP welcomed the different layers of redress mechanism provided in the PS, although it criticised the complexity and lack of clarity of the overall architecture that would, in its view, undermine the effective exercise of data subject's rights (opinion, p. 26).

in section 4.3.2 of this publication). In the second alternative, the DoC can consider refusal to cooperate as a persistent failure to comply, which leads to the organisation's removal from the PS list (after 30 days' notice). The DPAs can refer complaints to the DoC via a contact point. Upon receiving a claim, if the DPA considers that transfer to a company was in violation of EU data protection law, it can, if necessary, suspend the transfer of data.

(5) The PS firms are subject to US authority investigatory and enforcement powers, such as the FTC. Priority will be given to referral of non-compliance from independent dispute resolution bodies or self-regulatory bodies, DPAs and the DoC. Individuals will still be able to directly submit claims of non-compliance with section 5 of the FTC Act.

Figure 1 – Redress mechanisms available to individuals



Source: EPRS, 2017.

(6) As a **last resort**, the PS institutes a **Privacy Shield arbitration panel** if any of the above-mentioned recourse avenues have not resolved the individual complaint. It can only be invoked by individuals and is triggered by the data subject sending a formal notice to the company (indicating the steps already taken). The Privacy Shield panel will be made of one to three arbitrators, chosen by the DoC and the FTC among a pool of 20 arbitrators; the panel has authority to decide a non-monetary remedy (e.g. access, correction, deletion of data). While no monetary damages can be awarded by the panel (but are obtainable in court), data subjects can ask to **enforce the award in US courts** under the Federal Arbitration Act. **Arbitral costs** are taken from a dedicated fund (supplied with PS companies' contributions); if the individual decides to be assisted by a lawyer, the lawyer's fees are not covered by the fund.

(7) Claims can be brought directly under US laws which provide legal remedies under tort law, misrepresentation, unfair and deceptive practices,[103] and breach of contract.

4.3. The new US authorities' commitments and oversight mechanisms

4.3.1. *US Department of Commerce*

The Department of Commerce (DoC) reiterated its former commitments and added new ones to ensure the enforceability of the system. Under the Safe Harbour (SH), the DoC already had to list all self-certified organisations. The DoC has now stressed its commitment to keep the list updated by removing firms from the list which no longer comply with the Privacy Shield (PS) rules, or do not re-certify. The DoC has committed to notify firms of their removal from the list as well as verify whether firms that were removed or decided to withdraw from the PS delete the data received while participating with the PS, or whether they intend to keep that data, and if so, under what circumstances (whether they will continue to follow the PS principles and whether there is a contact point for that data). The list must also specify the data covered, in particular, whether the self-certifying company has registered for human resources data as those entail further obligations on the firm. The DoC has also to verify the requirements for self-certification; this includes verifying that all self-certified companies have registered with an independent resolution body, or verifying the public availability of the firm's privacy policy.

The DoC will now also address false claims of participation through:

(1) the review of organisations removed from the list and verifying that they no longer claim participation in the Privacy Shield;
(2) the review of organisations that need to be removed, either because they have not re-certified, have withdrawn, or are removed as for persisting failure to comply;
(3) undertaking any other effort to identify false claims;
(4) promptly addressing any issues that may arise or complaints that are received regarding false claims and taking corrective actions including pursuing legal pursuit.

The DoC will carry out compliance reviews of participating firms whenever it receives complaints, and/or an organisation does not respond to enquiries by the Department on implementation of the PS and/or there are credible doubts regarding the firms' compliance with the principles.[104] Finally, the DoC will establish dedicated contact points, both for enhanced cooperation with the DPAs as well as to receive referrals of data subjects' complaints on the implementation of the PS by a participating firm from DPAs.

4.3.2. *Federal Trade Commission*

Federal Trade Commission (FTC) action does not seem to have changed fundamentally. However, the FTC now has to give priority to claims of non-compliance referred by (a)

[103] See also C. Hoofnagle 'US Regulatory Values and Privacy Consequences', European Data Protection Law Review Vol 2 (2016), Issue 2, p. 169, who claims a need for more emphasis in US law on unfairness rather than on deceptiveness: this would be more in line with the EU data protection approach.

[104] The Article29WP welcomed the DoC investigatory powers in its April 2016 opinion, as well as the possibility to make *ex officio* verifications, in particular through sending questionnaires. However, it questioned the exact powers of US enforcement authorities to conduct on-site inspections at the self-certified organisations to investigate Privacy Shield violations, on how *exequatur* of an EU authority decision could be obtained on US territory.

independent resolution bodies; (b) European DPAs; (c) the DoC. As mentioned above, data subjects can always make direct claims to the FTC.

Box 6 – Federal Trade Commission and section 5 proceedings

The FTC's primary legal authority comes from section 5 of the FTC Act,[105] which prohibits unfair or deceptive practices in the marketplace. Section 5 of the FTC Act has broad application (at least as broad as the FTC jurisdiction, so it does not apply to sectors excluded from FTC jurisdiction).[106] FTC authority covers both cases of misrepresentation (i.e. cases where firms make deceptive statements and promises to customers) and cases where firms omit a material fact (this latter could also refer to data, for example in cases where the firm does not notify the consumer that it is gathering personal information on their account). The FTC actions under section 5 can be brought against any firm within its jurisdiction. Section 5 applies to actions occurring in the USA or having effects in the USA. In this light, section 5 can be used to bring complaints by EU citizens impacted by actions of a US firm (for example, in the Safe Harbour (SH) case *Best Priced Brand*,[107] action was taken against an US firm whose actions were directed at the United Kingdom market). However, FTC Commissioner Julie Brill stated that the invalidity of the SH framework lessened FTC enforcement capacity in transatlantic cases. This is true in as much as the SH framework obliged participating companies to issue clear and transparent privacy policy statements that were binding on the firms; not complying with such a statement could trigger FTC action; because the SH privacy statements were meant to be public and transparent, they eased FTC action in bringing forth a misrepresentation complaint. Sometimes actions under section 5 involved violation abroad.[108] The PS re-establishes that transparency and publicity requirement of the privacy policy of the firms, thus making claims to the FTC easier.

The FTC has two main procedures it can follow to bring a complaint before the courts.[109] The first, is to file a lawsuit in federal courts. This approach was used in the *Best Priced Brand* case mentioned above, for example. These approaches are often used in cases of fraud where the FTC wants to obtain a court order to freeze the assets of a company which might otherwise disappear before the investigation is finalised. The second route is internal and consists of investigation and administrative-type procedures (see for example the *Google, Inc., In the Matter of* case).[110] If the respondent does not comply with the order, the FTC can request penalty payments. This was the case in some of the SH cases brought by the FTC.[111]

4.3.3. *US intelligence agencies and law enforcement*

According to the Privacy Shield (PS), 'adherence to the principles may be limited to the extent necessary to meet national security, public interest or law enforcement requirements[...]'(annex II, I.5), therefore, allowing, in some circumstances, US public authorities to access and use (EU) personal data. Regarding the extent and justifiability of these derogations in a democratic society (one of the main issues at stake in the *Schrems* case), this assessment regards the US legal framework on data access by

[105] Federal Trade Commission Act.

[106] See footnote 9

[107] *Best Priced Brands, LLC, et al.*

[108] See for example the US *GMR Transcription Services* case, in which the US firm had outsourced data processing abroad, and privacy violations were perpetrated by the processor abroad; the FTC brought a case against the US firm as the latter was not capable of properly verifying the processor's actions.

[109] For more information on the procedures refer to the FTC website (last accessed 9 November 2016).

[110] See, for example, the SH case brought to the FTC in the *Google* case concerning the roll-out of social network Buzz.

[111] See for example, the *Facebook* case and the *Myspace* case.

intelligence and other US authorities mentioned in the annexes to the PS.[112] Commissioner Jourová assured that the Commission had addressed the opinions of the EP Resolution and the article 29 Working Party to further strengthen the safeguards in the PS. As regards the issue of bulk collection of data, the Commissioner confirmed having received further assurance from US authorities that bulk collection of 'signal intelligence' (e.g., gathering of communication signals)[113] by the US intelligence community will be exceptional and 'as tailored as feasible', when other measures are technically impossible (as mentioned in annex III, A; VI and VII of the PS).[114] These assurances allowed the Commission to conclude that the data processing remains within the limit of necessity and proportionality, as requested by the CJEU.

Concerning the oversight[115] and **redress mechanisms** in the context of data access by intelligence and law enforcement authorities, the Commission welcomed the new role of the Ombudsperson (annex III, A), who is obliged to respond to individual complaints with confirmation of compliance or remediation of non-compliance, and confirmed having received assurance of the Ombudsperson's independence from the intelligence community (however, see the Article 29 Working Party's statement in section 5.1.2.).

---

[112] These are: the Foreign Intelligence Surveillance Act (FISA), the Executive Order 12333, the USA Freedom Act, and the 2014 Presidential Policy Directive 28 (PPD-28), (although the latter is not a legal basis for collection).

[113] The Article29WP remarked in its opinion on the lack of definition of signal intelligences in any applicable text.

[114] In particular, the 2015 **USA Freedom Act** (consistent with the Fourth Amendment to the US Constitution), introduced minimisation rules for government access to data based on **FISA**, which for instance, at **section 702**, allows US intelligence agencies to conduct surveillance programs (like PRISM) and to seek access to information, including content of e-communications by non-US citizens located abroad who are supposed to be 'individually identified legitimate targets' and is subject to the PPD-28 requirements (annex VI). The **US PPD-28 of 2014** imposes limitations to signals intelligence operations by intelligence agencies, which may be collected exclusively where there is a foreign intelligence purpose and 'wherever practicable', and should be focused on specific foreign targets or topics through the use of discriminants or selectors (specific terms or identifiers, like email addresses). PPD-28 also stipulates that collection must be based on a statute and in accordance with the US Constitution, treating all persons with dignity. It also recognises that intelligence agencies may collect bulk signals in certain circumstances when the use of discriminants is not possible 'due to technical or operational considerations' in order to identify new threats, but as narrow as possible (i.e. focus on a territorial region) and using filtering tools to minimise the collection of non-pertinent data. The use of data thus collected would be limited to **six specific cases** of national security purposes (including counter-terrorism) that, however, in the Article29WP's view, are rather too wide to be able to remove the possibility of indiscriminate collection: '[under PPD-28] collection possibilities remain unclear and potentially broad' (Article 29 Working Party opinion, p. 38). In the representation made by the US Office of the Director of National Intelligence (ODNI) (annex VI of PS), the signals intelligence collected by US authorities would represent only a fraction of communications via the internet and bulk collection would not mean mass or indiscriminate collection of data. This is an aspect of debate (and often of divergence) between the EU and USA, because EU law considers data collection (not only access) as data processing subject to data protection rules (including consent or other legal grounds).

[115] For example, intelligence activities based on FISA allow for review and in some cases prior authorisation by the FISA Court (FISC), whose decisions can be challenged before the related Court of Review and ultimately the US Supreme Court; its control seems however limited to the condition that the purpose for the acquisition of data is to obtain foreign intelligence information and does not provide for effective judicial oversight on the targeting of non-US citizens (Article29WP opinion p. 43).

Box 7 – Redress avenues for undue access and use of data by US public authorities

In the case of redress avenues for undue access and use of data by US public authorities for national security purposes, the following are the main avenues open to individuals[116] mentioned in the EC's implementing decision on the PS:

(1) Under the Foreign Intelligence Surveillance Act (FISA), non-US citizens may have redress to challenge unlawful electronic surveillance.[117] Nevertheless, FISA's redress reach remains limited, and standing requirements for FISA claims have proved difficult to achieve. FISA is complemented by the Freedom of Information Act (FOIA), which allows individuals to seek access to federal agency records; however, the possibilities are limited, for instance by exceptions in case of classified national security information or those concerning law enforcement investigations.[118]

(2) Other specific legal bases exist under the Computer Fraud and Abuse Act, Electronic Communications Privacy Act and the Right to Financial Privacy Act. These avenues only refer to specific data, targets and types of access to the data. There is a more general administrative redress to seek judicial review whenever any person suffers 'legal wrong because of agency action, or adversely affected or aggrieved by agency action'.[119] However, there is no mention in the implementing decision regarding the level of proof required to make a case under this more general administrative redress.

(3) The Privacy Shield creates a new **Privacy Shield Ombudsperson** mechanism which should ensure that individual complaints are duly investigated and addressed. The Ombudsperson is assisted by (existing) independent investigation structures such as the Inspectors-General[120] and the Privacy and Civil Liberties Oversight Board (PCLOB), which was established as an independent bipartisan agency within the executive branch, and whose main role is to ensure that the US executive actions in the field of terrorism respect privacy and civil liberties,[121] and has statutory public transparency requirements.

[116] The need to clarify that redress mechanisms and rights are ensured for individuals whose data are transferred from the EU to the USA (i.e. including residents and not limited to EU citizens) is particularly urged by Article29WP in its April 2016 opinion (p. 14). See also the Commission guide for citizens.

[117] 50 US Code § 1810 – civil liability.

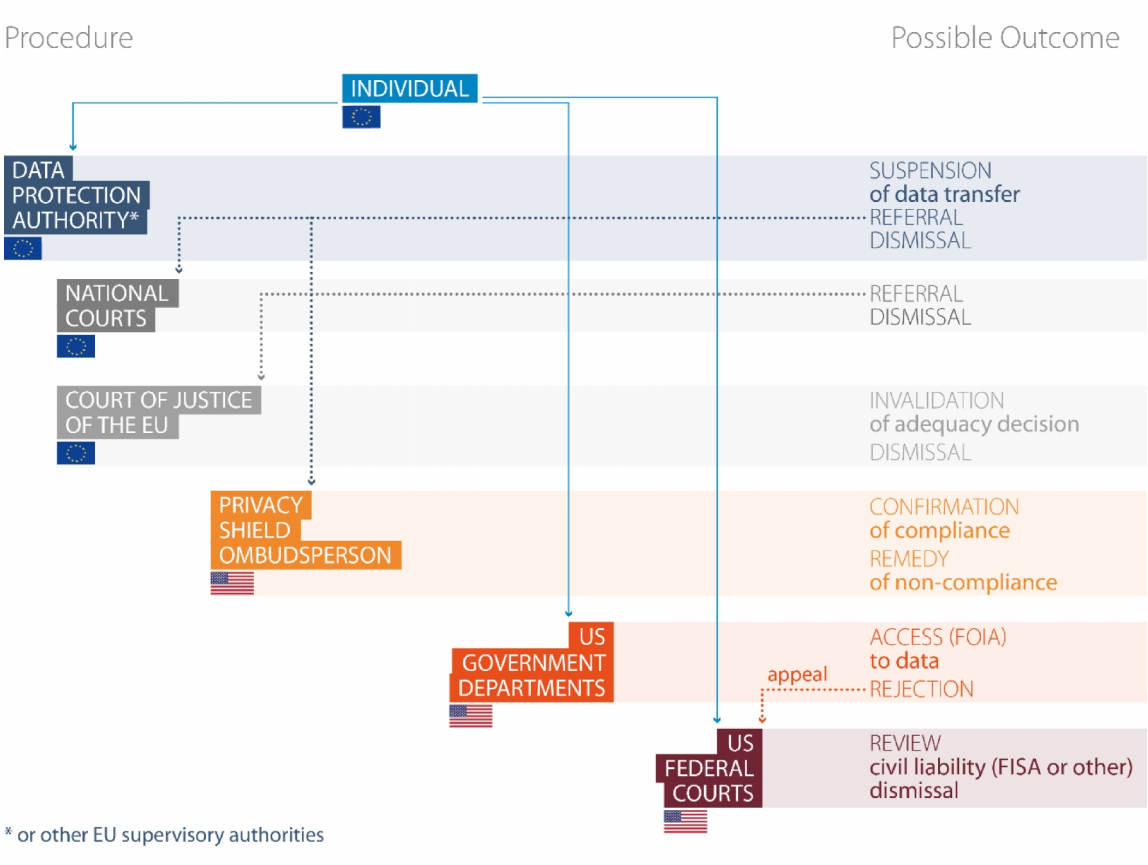
[118] The individual in these cases can only receive a reply in which the agency declares either to confirm or deny the existence of any records.

[119] Right of Review in the Administrative Procedure Act, 5 US Code § 702

[120] Inspectors General (IGs) are oversight offices within a US or federal state intelligence agency. They are in charge of audits, inspections and review of activities in the intelligence communities.

[121] Recommendations of the 9/11 Commission Act, Pub. L. 110-53, signed into law in August 2007 (codified in 42 USC §2000ee et seq.). A recent oversight review focused on surveillance programmes operated under section 701 FISA. It should be noted that PCLOB have access to all relevant agency records, reports, documents and other materials, including classified information consistent with the law (annex VI p. 96).

Figure 2 – Redress avenues for undue access and use by US public authorities



Source: EPRS, 2017.

5. Toward a satisfactory and enduring tool?

5.1. Reactions to the new version of the Privacy Shield

Different reactions have been registered in the aftermath of the adoption of the new arrangement. Most of the representatives of the commercial sectors in Europe and in the USA welcomed the new deal.[122] However, although formal adoption is concluded, this does not seem to be the end of the debate for many observers and policy-makers. Neither does the arrangement seem to completely pacify the criticisms still present in the aftermath of publication of the new Privacy Shield (PS).[123] In particular, the **long-term viability** of the PS as an instrument capable of effectively safeguarding privacy rights according to EU standards has still to be confirmed. Some EU policy-makers and consumer associations put this in doubt.

Moreover, criticisms pointed to a series of shortcomings.

[122] See statement by Digital Europe, voicing the European digital technology industry; also N. Drozdiak, 'The EU Agree on Final Adjustments to Data Privacy Shield', Wall Street Journal, 24 June 2016.

[123] For instance, Jan Philipp Albrecht (Greens/EFA, Germany, and also rapporteur for the GDPR) affirmed: 'The Commission has today signed a blank cheque for the transfer of personal data of EU citizens to the USA ....the Commission should not be simply accepting reassurances from the US authorities but should be insisting on improvements in the data protection guaranteed to European consumers'. Albrecht particularly criticised the fact that mass collection of personal data by the US surveillance authorities remains possible, despite the limitations set (six possibilities for access), and pointed out that PPD-28 is not equivalent to a US law and can be unilaterally withdrawn by any future US President. Jan Philipp Albrecht also claimed that the adequacy decision should be renegotiated when the new general DP regulation comes into force in early 2018.

5.1.1. *Privacy advocates*

As to the **commercial aspects**, the PS was considered to allow data processing for very broad and generic purposes, contrary to the purpose limitation principle as enshrined in EU law. Actually, the text of the PS requires firms to inform individuals of 'the purposes for which it collects and uses personal information about them'; it is, however, unsure how detailed such a purpose must be, the PS does not require the firms to specify the actual use for which the information is intended. Moreover, commentators have noted that the PS would be based on an 'op out' system (notice and choice), requiring users to actively object to their data being processed by a company (if they are aware of such processing), and **contrary to the EU 'opt in' system** that requires companies to obtain prior user consent. As to the redress system against a company, observers stress that the **mechanism remains very complex** and, notwithstanding efforts on the cost side, could remain inaccessible for EU citizens, (e.g., citizens would have to contact the company first, then locate and turn to different private arbitration bodies or national authorities, the FTC and the DoC, and, only after these attempts, the 'Privacy Shield panel', for a binding arbitration award); in case the company fails to comply with a judgment awarded by the new 'PS panel', this would need to be enforced by a court).[124]

Regarding the shortcomings in the **'surveillance'** sector, the main problem seems to be represented by the explicit reference to 'bulk collection' of data by the US authorities (annex VI), although its use is limited to six cases for (broadly defined) security purposes. As for the redress options in this sector, the Ombudsperson's role was seen as unsatisfactory for two reasons. First, it was considered that the office would not be able to fully address complaints of data surveillance by US authorities, as it will not be able to confirm or deny whether an individual has been subject to surveillance measures. This issue will remain covered by the FOIA only, although limited by specific exceptions. The Ombudsperson and the independent investigation authorities, working in collaboration with him, will therefore limit investigations to the assessment of whether action taken by intelligence agencies has violated the law. The second point raised by commentators is that the Ombudsperson would not be an independent court, but an Undersecretary of the US State Department. While this position could give the Ombudsperson easier access to some information to make an assessment of the activities under complaint, and while the PS mentions many times the Ombudsperson's independence, commentators did not see the required guarantees. Therefore, the office would not guarantee the right to an effective remedy and a fair trial, as requested by article 47 of the CFR.[125]

Similar criticisms were made by the **European Consumer Organisation** (BEUC), expressing disappointment that the PS would underpin the transfer of data without sufficiently protecting EU citizens. While a framework is considered necessary ('because the processing of personal data for commercial purposes remains largely unregulated in the USA'), the PS is deemed the product of political and commercial pressure from the

[124] See statement by Max Schrems, *Privacy Shield – Press Breakfast by Jan Albrecht MEP*, 12 July 2016.

[125] Ibid. Max Schrems still sees difficulties in the new PS with regard to blanket surveillance and especially with regard to intelligence agencies' access to certain data, even if this is limited – for example, on the grounds of terrorist threat. In his view, the definition is still too vague and he is also concerned by the difficulty for Europeans to appeal because the appeal mechanisms are particularly complex and could make a complainant wait 'for years'.

US technology industry and government, and fails to provide an adequate level of protection.[126]

5.1.2. *Article 29 Working Party and European Data Protection Supervisors*

The **Article 29 Working Party issued its statement** on the amended Privacy Shield adequacy decision two weeks after its publication,[127] in which the Group of European DPAs welcomed the improvements of the final version, but expressed a number of concerns that still remain on both commercial aspects and on the US public authorities' access to data. On the first point, the lack of specific rules on automated decisions is mentioned, as well as the right to object and the lack of clarity on how the new framework will apply to data processors. Regarding the derogations for security purposes and US public authority access to data, the Article 29 Working Party's concerns are to be found in the lack, under the new PS, of stricter guarantees on **the independence and power of the Ombudsperson**. Concerning the bulk collection of data (one of the main thorny points in the whole PS debate), the Office of the Director of National Intelligence (ODNI) made commitments not to conduct mass and indiscriminate collection of data; however, EU DPAs expressed concern regarding the fact that **concrete assurances** to prevent this sort of surveillance could not be found in the PS.

The crucial moment for assessing the efficiency and robustness of the PS, according to the Article29WP, is the **first joint annual review** (planned to take place by summer 2017). The aim of the review should be, according to the Article29WP, to verify if the remaining issues have been solved and also if safeguards provided under the PS are effective. It should be noted that the results of the first joint review are supposed to also have an impact on other transfer tools such as BCR and SCC, by confirming their legal strength.[128] Additionally, the WP committed itself to proactively **assist data subjects** when dealing with complaints, to provide suggestions to data controllers to comply with their obligations under the PS. Finally, the Article 29 WP appeared willing to give the new PS a chance (backing Commissioner Jourová's claim), but according to a **cautious approach**, rather than a true endorsement (at least in view of the expected annual review).

The importance given by commentators on the PS to the existence of oversight mechanisms and effective and agile redress systems, can be better understood through the words of the **EDPS** Giovanni Buttarelli: 'There has been an exponential rise in the

---

[126] BEUC, press release, 12 July 2016, 'Privacy Shield opens hole in protection of EU citizens' privacy', reporting declarations by BEUC's Director, Monique Goyens, according to whom, by not defending its data protection rules properly, the Commission has allowed commercial motivations to outweigh citizens' rights to privacy ('Consumers usually do not know or control where companies are sending their personal data'). Although some improvement is recognised, the overall structure and value of the consumer redress mechanisms are considered messy and complex; and a legal challenge in front of the court is not excluded: 'A fundamental problem remains that the US side of the shield is made of clay, not iron'.

[127] See Article29WP statement on the Decision of the European Commission on the EU-US Privacy Shield. Moreover, Article29WP pointed out the lack of clarity on the use of cable interceptions by US intelligence for data in transit to the US, on the legality of which there is, so far, no established jurisprudence. Also the concept of signals intelligence is not defined in any applicable text.

[128] Practical organisation of the joint review as well as the DPAs' competence during the review are expected to be clearly defined: in the same statement, the Article29WP calls for all the members of the review team to have the possibility to access all the information necessary for the review, i.e. to allow also for verification of necessity and proportionality of the collection and access to data by public authorities).

volumes of personal data being collected, stored, and transferred, which information is increasingly not provided by the individual him- or herself, but rather observed, derived, or computed by someone else. For human rights to have any meaning, it is therefore essential for someone to be responsible for how that data are used'.[129] Moreover, regarding the 'likely longevity' of the Privacy Shield, he claimed that 'we need a robust model for how bilateral data sharing agreements can work .... Similar exercises to that ongoing between the EU and USA may now be needed between other trading partners'. Giovanni Buttarelli's hope is ultimately that, with the **GDPR** fully in force (2018), 'we will be able to achieve a common standard, a sort of a digital gold standard which will accompany globalisation and all the benefits and challenges it poses for individuals and society'.[130]

5.2. Outlook

Although the Privacy Shield (PS) can be said to be formally completed, this is not the end of the story.

- Firstly, the joint **annual review**, as indicated, is expected to take place by summer 2017.
- Although the new text of the PS already contains aspects not covered by the Data Protection Directive in order to be in line with the GDPR (such as onward transfers of data), an assessment of the PS is also expected when the **GDPR** fully takes effect, in **May 2018**, to make, if required, the necessary improvements.[131]
- The **EP** is expected to adopt a **new resolution** on the PS in the near future.[132]
- Regarding **attitudes of companies**, (which may decide to stick to alternative tools): on a practical level, some scholars[133] suggest that in the near future companies could also be proactive, by implementing data minimisation and anonymisation (therefore reducing the cases of data processing subject to the EU data protection rules). Companies also seem to have been rather cautious in subscribing to the PS; at the end of October 2016, about 1 500 companies had submitted certification (500 of which were certified by the DoC on 18 October 2016).[134] This number is much smaller than the 4 000 companies that were registered under the Safe Harbour (SH). There

---

[129] Giovanni Buttarelli, 'The EU GDPR as a clarion call for a new global digital gold standard', Guest Editorial, *International Data Privacy Law,* Oxford Journals Law, 2016, Vol 6 (2), pp. 77-78. He also stressed that 'Individuals are subject to granular inferences drawn from statistics through advanced analytics based on algorithms of which they are at best only partially aware. They are put at risk by data processing which is unfair or discriminatory and which entrenches stereotypes and social exclusion. Accountability should promote sustainable data processing, by ensuring that the burden of assessing the legality and fairness of complex processing falls primarily on controllers and regulators, not on the individual'.

[130] *Ibid*.

[131] As stressed by G. Buttarelli, cit., the CJEU 'applies these rules [GDPR] strictly, interpreting them in light of the EU CFR and favouring the rights and interests of the individual above corporate or business aims, however reasonable and legitimate'.

[132] A draft motion for a (new) resolution on the adequacy of the protection afforded by the EU-US Privacy Shield (expressing some persisting concerns) was discussed in the LIBE Committee in the first meeting of 2017.

[133] See A. Montelero, cit.

[134] US Department of Commerce marks posting of 500th company on Privacy Shield Framework list, International Trade Administration (ITA), 18 October 2016.

might be several explanations for this: (1) the time needed to adapt and understand the rules before applying for certification, (2) firms are cautious, and may fear new challenges to the PS, when the PS seems more costly to implement than the SH.

- The TTIP negotiation discussions on data flows were temporarily suspended while the EU and the USA were negotiating a solution to the EU-US data protection issues including the PS. With the adoption of the Commission's adequacy decision on the PS and approval by Member States on 8 July 2016, discussion on e-commerce and data flows can be resumed. Provisions allowing for data transfers are an integral part of certain chapters of trade agreements, in particular in the financial services and digital services.[135] These provisions contain special exceptions allowing for adequate safeguards to protect privacy.[136] The EU also introduces privacy policy regulations as part of the general exceptions of other agreements.[137]
- Moreover, if not directly, the PS may soon also be taken into account in relation to data transfers to **other third countries**.[138]
- In addition, the *Schrems* decision and its consequences are expected to be relevant in other CJEU cases, as happened recently in the case of the EU-Canada Passenger Name Records (PNR) agreement.[139]
- Another issue that has recently emerged and which needs further discussion, concerns the consequences of **'Brexit'**[140] on the PS and on triangular data flows between the USA, the United Kingdom (UK) and the EU. The uncertainty created by Brexit could continue for two years (or even longer) from the moment of notification under Article 50 TEU of the UK decision to leave the EU. The PS will apply to the UK as long as it formally remains part of the EU. In the case of a UK exit from the EU, cross-border data transfers would be similar to those with other third countries.[141] In the case that the EU and UK choose the option of applying EEA law to their relationship, then the PS would have to be implemented in the UK, as the GDPR.

---

[135] On this aspect see also the study by K. Irion et al, 'Trade and privacy: complicated bedfellows? How to achieve data protection-proof free trade agreements', commissioned by BEUC et al., July 2016, Amsterdam, Institute for Information Law (IViR).

[136] On this aspect, see the EP LIBE Committee's opinion of April 2015, with the recommendation that the agreement envisages an unambiguous horizontal exception for EU data protection law.

[137] In CETA, for instance, data protection is mentioned in several chapters, but see, for example, article 13.15 CETA on financial services, and on general exceptions, article 28.3 CETA.

[138] On this point, the Commission published recently a communication on Exchanging and Protecting Personal Data in a Globalised World, setting out its strategy for new adequacy decisions on data transfers to third countries (such as Japan and Korea) and indicating as well alternative data transfer mechanisms.

[139] See the Advocate General (AG) of the CJEU (Mengozzi) opinion on the draft **EU-Canada PNR agreement**. The EP asked the CJEU for a preliminary verification of the agreement in November 2014, before a final vote in plenary. The AG seemed to confirm the EP's concerns regarding its compatibility with the European Charter. See also the EDPS plea in the hearing of 5 April 2016.

[140] The term Brexit refers to the withdrawal of the UK from the EU, the outcome of a recent referendum.

[141] In the first case, an adequate level of data protection should be ensured for companies to be able to make EU-UK data transfers. However, there are several reasons to believe that UK will abide by European data protection rules (see UK Information Commissioner's declaration), so enactment of an adequacy decision to allow EU-UK data flows could be a formality. See also Christopher Kuner, 'The global data protection implications of 'Brexit'', International Data Privacy Law, 2016, vol 6, No 3.

- Finally, the Privacy Shield could be brought in front of national and European courts by individuals, European DPAs[142] or privacy advocacy associations, with regard to its adequacy. Indeed, recourse has recently been made by Digital Rights Ireland to the General Court (the lower Court of the CJEU).[143]

6. Main references

Bender D., Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective, International Data Privacy law, 2016, Vol 6, No 2

Boehm F., A comparison between US and EU data protection legislation for law enforcement purposes, Directorate General for Internal Policy – European Parliament, September 2015.

Brill J., Strengthening International Ties Can Support Increased Convergence of Privacy Regimes, European Data Protection Law Review, Vol 2 (2016).

Determann L., Adequacy of data protection in the USA: myths and facts, International Data Privacy Law, 2016, Vol 6, No 3.

Fielder A., From an unSafe Harbour to a Privacy Shield full of holes, Privacy International, April 2016

Hoofnagle C., US Regulatory Values and Privacy Consequences, European Data Protection Law Review Vol 2 (2016), Issue 2.

Irion K., et al, Trade and privacy: complicated bedfellows? How to achieve data protection-proof free trade agreements, commissioned by BEUC et al., July 2016, Amsterdam Institute for Information Law (IViR).

Kuner C., Extraterritoriality and regulation of international data transfers in EU data protection law, International Data Privacy Law (2015), 5 (4).

Resta G. – V. Zeno-Zencovich (*eds*), La protezione transnazionale dei dati personali. Dai 'SH Principles' al 'Privacy Shield', Roma Tre Press, 2016.

[142] The Hamburg DPA, for instance, seems willing to ask the CJEU to check the validity of the new Commission decision.

[143] As Reuters reported, the challenge against the Privacy Shield adequacy decision (T-670/16) was filed by the DRI against the European Commission on 16 September 2016. In its action, DRI claims that the Privacy Shield is 'a manifest error of assessment by the Commission', alleging that: the privacy principles and the official commitments contained in the annexes to the PS would not constitute 'international commitments' in the meaning of Directive 95/46/EC; that the FISA would permit US public authorities to have secret access on a generalised basis to e-communications; that ultimately the contested decision would fail to adequately ensure that the EU citizens' rights are fully provided for where their data are transferred to the USA.

The CJEU's *Schrems* judgment of October 2015, besides declaring the European Commission's Decision on the EU-US 'Safe Harbour' data transfer regime invalid, has also settled a number of crucial requirements corresponding to the foundations of EU data protection. In the assessment of the Privacy Shield, the new framework for EU-US data transfer, these need to be taken into account.

In less than one year since the CJEU ruling, the Commission has adopted a new adequacy decision, in which the Privacy Shield regime is deemed to adequately protect EU citizens. The main improvements of the Privacy Shield (over its predecessor), as well as the critical reactions to the new arrangements, are discussed in this analysis, taking into account, however, that an annual review is expected to take place by summer 2017, which will also take into account the coming into effect of the EU General Data Protection Regulation in 2018.

QA-06-16-293-EN-N

This is a publication of the
Members' Research Service

Directorate-General for Parliamentary Research Services, European Parliament

PE 595.892
ISBN 978-92-846-0369-5
doi:10.2861/09488

The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to the Members and staff of the EP for their parliamentary work.