European Parliament

The Privacy Shield

Update on the state of play of the EU-US data transfer rules

IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service

Authors: Shara Monteleone and Laura Puccio
Members' Research Service

PE 625.151 – July 2018

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. The first joint annual review of the Privacy Shield took place in September 2017, but concerns still remain to be addressed as expressed by the European Parliament in its recent resolution on the adequacy of the Privacy Shield. This paper aims to present recent developments and is an updated version of one published in January 2017: PE 595.892.

AUTHOR(S)

Shara Monteleone and Laura Puccio

This paper has been drawn up by the Members' Research Service, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

To contact the authors, please email: eprs@ep.europa.eu

LINGUISTIC VERSIONS

Original: EN

Translations: DE, FR

Original manuscript, in English, completed in January 2017.

This updated edition was completed in July 2018.

PE 625.151
ISBN: 978-92-846-2234-4
DOI:10.2861/675548
CAT: QA-07-17-018-EN-N

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 regime invalid. This regime had formed the legal basis to allow transfers of data, 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 relied is that of 'equivalence' – between the level of protection existing in a third country, and the European data protection system. The Court invalidated the Commission's Safe Harbour adequacy decision as it did not contain any findings regarding the existence in the USA of laws and practices limiting interference on the right to privacy and data protection (e.g. interference by public authorities for security purposes), nor of effective judicial remedies for individuals. According to the judgment, laws which establish exceptions (such as enacting measures for security purposes) which could 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 the 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 could be part of an adequate data protection system, it should be accompanied by effective enforcement and oversight mechanisms.

As a consequence, the judgment ruled the Safe Harbour framework, on which a large number of companies had relied, insufficient to ensure the high level of protection for EU citizens required under EU law. This invalidation of Safe Harbour 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.

In 2016, the European Commission and the USA adopted a new framework for transatlantic exchange of personal data, known as the **Privacy Shield**. Within a year, more than 3000 companies had subscribed to the new framework, and the US Federal Trade Commission had already triggered three cases of non-compliance with Privacy Shield. In September 2017, the first joint annual review of Privacy Shield took place. Although considered to be working well, a number of recommendations for further improvements were issued. Moreover, a range of concerns still remain to be addressed (not least in view of the recent Facebook / Cambridge Analytica scandal). The European Parliament adopted a resolution in July 2018, which, although acknowledging some improvements, reiterates a number of persistent concerns on Privacy Shield, and calls on the Commission to suspend the Shield.. Unless the concerns can be resolved satisfactorily, the underlying legal uncertainty may not disappear, and Privacy Shield is also likely to end up challenged before the CJEU, like its predecessor.

Table of contents

1. Introduction 1

2. EU policy on data transfer and the *Schrems* case 1

2.1. High level of EU data protection and third countries 1

2.2. Court of Justice of the EU: *Schrems* case and its consequences 3

2.3. The post-*Schrems* transition 6

2.4. Post-*Schrems* reactions 8

3. Revised Privacy Shield 10

3.1. Privacy principles and firms' obligations 12

3.2. New redress mechanisms 14

3.3. The new US authorities' commitments and oversight mechanisms 17

3.3.1. US Department of Commerce 17

3.3.2. Federal Trade Commission 17

3.3.3. US intelligence agencies and law enforcement 18

4. Towards a satisfactory and enduring tool? 20

4.1. Reactions to Privacy Shield 20

4.1.1. Privacy advocates 21

4.1.2. Article 29 Working Party and European Data Protection Supervisor 22

4.1.3. The European Parliament resolution of April 2017 23

4.2. Initial implementation and way forward 23

4.2.1. Initial Implementation 23

4.2.2. Review and outlook 24

4.2.3. The Facebook/Cambridge Analytica scandal and the latest EP resolution 27

4.2.4. Privacy Shield and other countries 29

5. Main references 32

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 of protection when data are transferred outside the European Economic Area (EEA). As a result, a new framework for governing transatlantic data flows became urgent.

The Commission and US authorities discussed a new framework to replace Safe Harbour, Privacy Shield, and the Commission adopted the related adequacy decision on 12 July 2016. Although Privacy Shield has now been in place, and in use for a couple of years, a number of issues remain to be resolved before the desired level of legal certainty for companies and citizens can be ensured. These developments, 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 EU's General Data Protection Regulation, GDPR[2] (like the earlier European Data Protection Directive (DPD) 95/46/EC[3] which it replaced in May 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 45 GDPR and 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.

[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] 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).

[3] 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.

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

The procedure under GDPR is mainly the same as under the previous directive, although the assessment criteria are now specified. The European Commission assesses the level of data protection in the third country through an examination procedure (Articles 25(6) and 31(2) of the DPD; Art 45 (5) and 93 GDPR). Such adequacy was 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 according to Article 25 (2) DPD;[4] this assessment should now, under GDPR, take into account elements such as the respect for fundamental rights and freedoms, relevant legislation, including on national security, and the implementation of such legislation.[5] The Commission proposal is approved under comitology rules, within the Article 31 Committee made up of representatives of Member States.[6] 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 the basis of the rules contained in Article 25 DPD, 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.[7]

Box 2 – Former Safe Harbour protection

United States data controllers complying with SH principles[8] 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.[9]

---

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.'

5 See GDPR Article 45(2) as discussed on page 31 of this paper.

6 See Article 5 of Regulation (EU) No 182/2011 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 L 55, 28.2.2011, pp. 13-18.

7 For the full list of Commission adequacy decisions, refer to the Directorate-General for Justice Website.

8 Issuance of SH principles and transmission to European Commission, Federal Register 24 July 2000 and 19 September 2000.

9 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.[10] Indeed, as the SH principles functioned like promises to customers, failure to comply with such promises could trigger a case of unfair and deceptive practices pursuant to section 5 of the Free Trade Commission Act.[11]

The European Commission has recognised the emerging 'inadequacy' of the SH since 2013. In a 2013 review of the SH framework by the Commission,[12] 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[13] in 2013 about the US National Security Agency's mass surveillance programmes (e.g. PRISM)[14] 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,[15] 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 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

[10] 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.

[11] 15 US Code §45

[12] 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.

[13] E. Macaskill and G. Dance NSA files: decoded, *The Guardian*, 1 November 2013.

[14] 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.

[15] 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*.

framework under which the transfer occurred.[16] 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,[17] the CJEU, meeting in Grand Chamber, confirmed Advocate-General Bot's opinion,[18] 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. 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 this before the national courts, to have the issue referred to the CJEU;[19]
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. 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 (otherwise the same requirement would be easily circumvented).[20] 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). This also implies a continuous assessment of the rules and practices of third countries in terms of safeguards;[21]
3) derogations for security purposes should be strictly necessary and proportional. The number of derogations envisaged under the SH principles,[22] such as those for law enforcement and national security purposes,[23] 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

[16] 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?'.

[17] Case C-362/14 *Maximilian Schrems v. Data Protection Commissioner*, of 6 October 2015.

[18] See Opinion of Advocate General Bot delivered on 23 September 2015.

[19] 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.

[20] 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).

[21] 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.'

[22] See A. Mantelero, *'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.

[23] 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; ...'.

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.[24]

The Court declared – as the only instance entitled to do so – the related Commission adequacy decision to be invalid.[25] 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.)[26]

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. 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 of law enforcement and intelligence authorities to access data, as well as the redress system.

One of the consequences of the *Schrems* case[27] in the US legal system is precisely the resumption of the discussion on the **Judicial Redress Act (JRA)** in the US Congress.[28] 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). The EU considered the adoption of the **US Judicial Redress Act** (enacted in February 2016) as a prerequisite for the conclusion of the **umbrella agreement**,[29] on data transfers to the USA for law enforcement purposes,[30] which establishes 'for the first time, data protection as the basis for information sharing'.[31]

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

[24] 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.

[25] For a deeper analysis of the case see S. Monteleone & L. Puccio From Safe Harbour to Privacy Shield: Advances and shortcomings of the new EU-US data transfer rules, EPRS, 2017 and, by the same authors, The CJEU's Schrems ruling on the Safe Harbour Decision, EPRS 'At a glance' note, 2015.

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

[27] 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.

[28] Judicial Redress Act of 2015.

[29] See S. Monteleone, EU-US Umbrella Agreement on data protection, EPRS, 2016.

[30] In accordance with Article 218 TFEU, on 1 December 2016 the EP gave its consent to the conclusion of the umbrella agreement by the Council, which adopted its authorising decision the following day. The agreement entered into force on 1 February 2017.

[31] 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.

foreign signals intelligence by **Presidential Policy Directive 28** PPD-28 (2014),[32] are, as discussed below, 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.

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 law, including: (a) to clarify that safeguards apply to all individuals (independently from their nationality); (b) to ensure that judicial redress provisions are effective within the meaning of the CFR; and (c) to clarify that transfers of sensitive data in bulk are not authorised.[33]

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, for instance, the right to access to their data, the right of rectification, and erasure) would not respect the right to effective judicial protection as enshrined in Article 47 of the CFR (§95 of the judgment).[34]

Finally, it is worth noting that this ruling should be inscribed within the body of jurisprudence of European and national courts that have been called upon to interpret and apply laws in various cases concerning new technologies[35]. With the advances in digital technologies, and their increasing use in recent years in our daily lives – and with the correlated increasing numbers of disputes on the impact of these technologies on fundamental rights – the role of courts in policy and law-making has being growing.[36]

2.3. The post-*Schrems* transition

The EU and the USA are extremely interconnected markets, with trade flow values over US$1 trillion annually.[37] 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.[38] Over 4 000 companies relied on the SH

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

[33] EDPS, Preliminary Opinion.

[34] On this point, from Germany, the **Schleswig-Holstein** DPA (ULD) was particularly critical in its position paper after the judgment: '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'. See 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 even alternative means such as the data subject's consent cannot be easily invoked as a legal basis, because for consent to be freely given, it would require that comprehensive information is provided, including on the risks related to the derogations in favour of the US authorities. Other national DPAs have issued their own positions on the 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.

[35] Inter alia, S. Monteleone, Ambient Intelligence and the Right to Privacy: The Challenge of Detection Technologies, EUI Law Working Papers no 2011/13,

[36] See M. Brkan & E. Psychogiopoulou (eds.), *Courts, Privacy and Data Protection in the Digital Environment*, Elgar, 2017.

[37] G. Sabbati and C.F. Guidi, US: Economic indicators and trade with the EU, EPRS/Globalstat, July 2018.

[38] 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

adequacy decision for their transatlantic data transfers. Small and medium-sized enterprises also relied on SH for cross-data transfers.[39]

By declaring the Commission adequacy decision **invalid**, the CJEU made clear that data transfers to the USA based on the SH principles would no longer be in compliance with EU law. As a consequence, companies previously relying on the SH for their transatlantic data flows faced several issues.[40] 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.[41]

- The **first issue** concerned the impact on data transfers performed under SH prior to the CJEU ruling. The Article29WP[42] 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),[43] 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 could still take place on the basis of alternative grounds, namely the data subject's consent,[44] or if the data controller adduces appropriate safeguards, including by means of contractual clauses. See corresponding provisions in Article 46, 47 GDPR.
- The **third issue** concerned the establishment of a transitional period for firms to adjust.

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 wishing 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). The Article29WP considered the use of those tools to allow data flows in the aftermath of the *Schrems* case.

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.[45] Normally, this responsibility is

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: 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.

39 *ibid.*

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

41 Statement of the Article 29 Working Party.

42 Article29WP was an independent advisory body on data protection and privacy set up under Article 29 of the Data Protection Directive 95/46/EC, made up of EU national data protection authorities. It has been replaced by the European Data Protection Board, established by the GDPR (Articles 68-76).

43 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.

44 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.

45 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.

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 it to nominate a single entity in the EU/EEA, it can propose other mechanisms of liability that better fit the organisation.[46]

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 repealed DPD and Article 46 GDPR). 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 in Article 31(2) of the DPD and now Article 93 GDPR, 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 out by the Commission,[47] lay down obligations for data exporters and importers, including 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 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.

2.4. Post-*Schrems* reactions

The CJEU ruling triggered heated debate in the EU and elsewhere.[48] This section reports the main pertinent 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, with the US authorities, to overcome the situation

[46] 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.

[47] '(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).

[48] 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.

of uncertainty, including obligations on oversight mechanisms, transparency, proportionality and means of redress.[49]

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 SH regime, but have reaffirmed their power to carry out controls on the lawfulness of data transfers by data exporters.[50] 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 had 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.[51]

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'.[52] In particular, they pointed to the CJEU emphasis on the requirement that a third country should ensure effective protection and on the admissibility of limitations to data protection only when strictly necessary.

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.[53]

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.[54] In the aftermath of the CJEU ruling, the case and its consequences were debated in the EP.[55] On 29 October 2015, a follow-up to the 2014 resolution was adopted,[56] in which the EP also stressed the significance of the other CJEU ruling[57] 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

---

49 Article 29 Working Party Statement of 16 October 2016.

50 Among the first reactions to the *Schrems* ruling, **the Schleswig-Holstein DPA (Germany)** issued a position paper on 14 October 2015. As for other DPAs, the Italian **Garante** ruled that 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.

51 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.

52 See the joint letter, p. 8.

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

54 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.

55 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'.

56 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.

57 See footnote 25.

of surveillance'.[58] The reciprocal reference between the two courts on data protection matters (and its timing) is particularly meaningful.[59]

In its 2015 follow-up resolution, the EP also considered reforms made in the USA to surveillance legislation were significant for the development and implementation of the new framework, in particular the adoption of the US Judicial Redress Act.[60] Regarding democratic oversight, the EP mentioned that: 'While fully respecting that national 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.'[61]

3. Revised Privacy Shield

The Commission and the US Department of Commerce had been reviewing the SH framework for at least two years before *Schrems,* and negotiations then intensified. A substantial part of the negotiations were represented by an exchange of information between both sides of the Atlantic on how the US data protection system works.[62] On 29 February 2016, the Commission released a package of documents in order to comply with the *Schrems* judgment, constituting the **first version of the new EU-US Privacy Shield (PS) framework**.[63]

---

58 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', 2017. The CJEU is therefore expected to also apply the same reasoning of the ECtHR in future when assessing the validity, under the CFR, of other EU and Member State legislative acts in this same field.

59 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.

60 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 conclusion of the umbrella agreement is the adoption of the Judicial Redress Act in the US Congress; and: '... 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'.

61 *Ibid*. paragraph 20.

62 As a 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 for Citizens' Policies and Constitutional Affairs for the LIBE committee.

63 The package included: (a) a communication from the European Commission to the EP and the Council: 'transatlantic data flows: restoring trust through strong safeguards; (b) the European Commission draft adequacy decision; (c) the 'privacy principles' as released by the US Department of Commerce (DoC); (d) 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). See European Commission press release of 29 February 2016.

Concerns were raised on this first version of the PS by the media[64] as well as during a hearing organised by the EP's LIBE committee,[65] in particular pointing to the fact that it would still allow US intelligence to collect data massively and indiscriminately and use them in at least six specific cases,[66] and that new challenges could be brought to the court. The Article29WP **assessment** of the draft adequacy decision (as required by Article 25 DPD) was released on 13 April 2016.[67] The Article29WP opinion contained recommendations for improving the draft decision. In particular, the **lack of clarity** in some parts of the Commission's adequacy decision, the **doubtful independence of the proposed US ombudsman**, the remaining **possibility for 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 improvements with regard to data retention and purpose limitation principles, as well as to automated individual decisions and onward transfers. Finally, on US public authority access to data transferred under PS,[68] the main criticisms focussed 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.[69] Moreover, as regards the **judicial remedies**, the Article29WP noted 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 one, where anyone can go to court if they have a legitimate reason to suspect interference with their fundamental rights.[70] In addition, the US requirement appears thwarted by the lack of notification to individuals subject to surveillance measures even after they have ended.

The **European Parliament** (EP), which has no voting power in Commission implementing decisions, voiced its concerns regarding the new framework by adopting a first (non-binding) **resolution** on 26 May 2016,[71] in which it called upon the Commission to 'implement fully the recommendations expressed by the Article29WP, in order to reach a robust Privacy Shield'.

---

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

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

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

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

68 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.

69 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 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).

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

71 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 proposed by different political groups were rejected. Many MEPs questioned whether the PS would stand up in court, and left wing MEPs, led by Jan Philipp Albrecht (Greens/EFA, Germany), proposed to include a 'sunset clause' as a minimum requirement in 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.

In its **opinion** of 30 May 2016, the EDPS considered that the draft decision did not fully assess the possibilities for individuals to exercise their rights of access, rectification or erasure concerning data collected by public authorities for purposes other than national security (e.g. law enforcement or other 'public interest' purposes). While recognising that several levels of oversight and redress exist in the US, the EDPS underlined that they do not cover all potential cases of government access to personal data. Moreover, it considered that the wide number of exceptions in PS had to be limited.[72]

Concerns expressed in the EU prompted modifications to the draft adequacy decision. After some delay, on 8 July 2016, representatives of **EU Member States** (Article 31 committee) voted for the adoption of the PS package.[73] The new, amended decision, establishing that the new EU-US framework provides for adequate protection for European citizens' data, was **finally adopted** on **12 July 2016**.[74] 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's Official Journal, although a further couple of weeks was allowed for companies to 'transit' to the new regime. The new regime has thus now been fully operational for two years.

Among the changes promised, and in line with the CJEU's *Schrems ruling*, 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.

In parallel, the Commission released a **guide to the EU-US Privacy Shield**.[75]

3.1. Privacy principles and firms' obligations

Beginning from 1 August 2016, US-based companies 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 a specific **website**.[76]

While these principles appear similar to the SH principles, the new PS developed them to include a number of changes in the obligations on companies that these principles entail.[77]

The first principle of **notice** requires organisations to provide a series of information to individuals, including the purposes of data collection and use. While this principle is maintained in the PS, it also includes an obligation to make privacy policies public (indicating that they conform to the PS

---

72 EDPS Opinion 4/2016

73 See the formal vote of the Article 31 Committee.

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

75 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 nationality).

76 See Privacy Shield Framework.

77 For a comparative analysis with the Safe Harbour principles see the previous edition of this paper: S. Monteleone & L. Puccio From Safe Harbour to Privacy Shield: Advances and shortcomings of the new EU-US data transfer rules, EPRS, 2017.

principles),[78] and an organisation has to provide links to these and further information to the DoC. Moreover the principle now includes designation of an independent dispute-resolution body to address complaints. Originally, the principle of notice was not applicable to transfer to a third party acting as agent under the instruction of a company. This exception was changed in the new PS, so that 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** requires 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. Currently, PS allows opt-outs where a new 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 of their opt-out right; the PS clearly gives data subjects the right to object at any time for direct marketing purposes only,[79] while remaining silent on other cases of opt-out.[80]

The third principle on **onward transfers** (transfers to third parties) deals with disclosure of data to a third party. 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.[81] 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 an equivalent level of protection as guaranteed by the principles of the PS.[82] 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 that the data subject had authorised. This requirement applies to **all third-party transfers irrespective of their location**.[83] 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 necessary steps 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.

---

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

79 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.

80 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.

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

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

83 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).

Access to personal information held by an organisation has to be given to the data subject. **The PS recognised this right of data subjects**, who 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 on access is necessary and duly justified; and (3) the burden of proof rests on the organisation to prove that such requirements are fulfilled.[84] On the question of **automated decision-making** based on **automated processing**,[85] the PS adequacy decision, 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).[86] It further suggests the need to discuss profiling, which is covered in the GDPR; exchanges on this issue formed part of the first annual review (see below).

The PS **reinforces the security requirement**, by asking for reasonable and appropriate security measures to be put in place to protect data. 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 that a contract is concluded with any sub-contractors, guaranteeing the same level of protection.

The sixth principle, **data integrity** of personal information, requires data collected to be relevant for the purposes for which it was intended, and that the organisation ensures that data is reliable, accurate and complete. The PS also includes the **purpose limitation principle**. This principle states that organisations cannot process data for purposes incompatible with 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 this 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,[87] 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 its privacy policy; firms are instead obliged to mention the purpose for which the data is collected.

3.2. New redress mechanisms

Privacy Shield (PS) develops the **redress avenues and enforcement obligations**. In particular it makes cooperation with DPAs obligatory for participating organisations that process **human resources data**. For other organisations, cooperation with DPAs remains optional; 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

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

[85] 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.

[86] 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 PS. On enforcement issues in data protection in general see D. Wright & P. De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Springer, 2016.

[87] 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*).

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**.[88]

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 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 resolution body must provide information regarding 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 to, or accepts to, cooperate. Obligation to cooperate with the DPA is only imposed on PS-using 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 in section 3.3.2 of this paper).[89] 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.

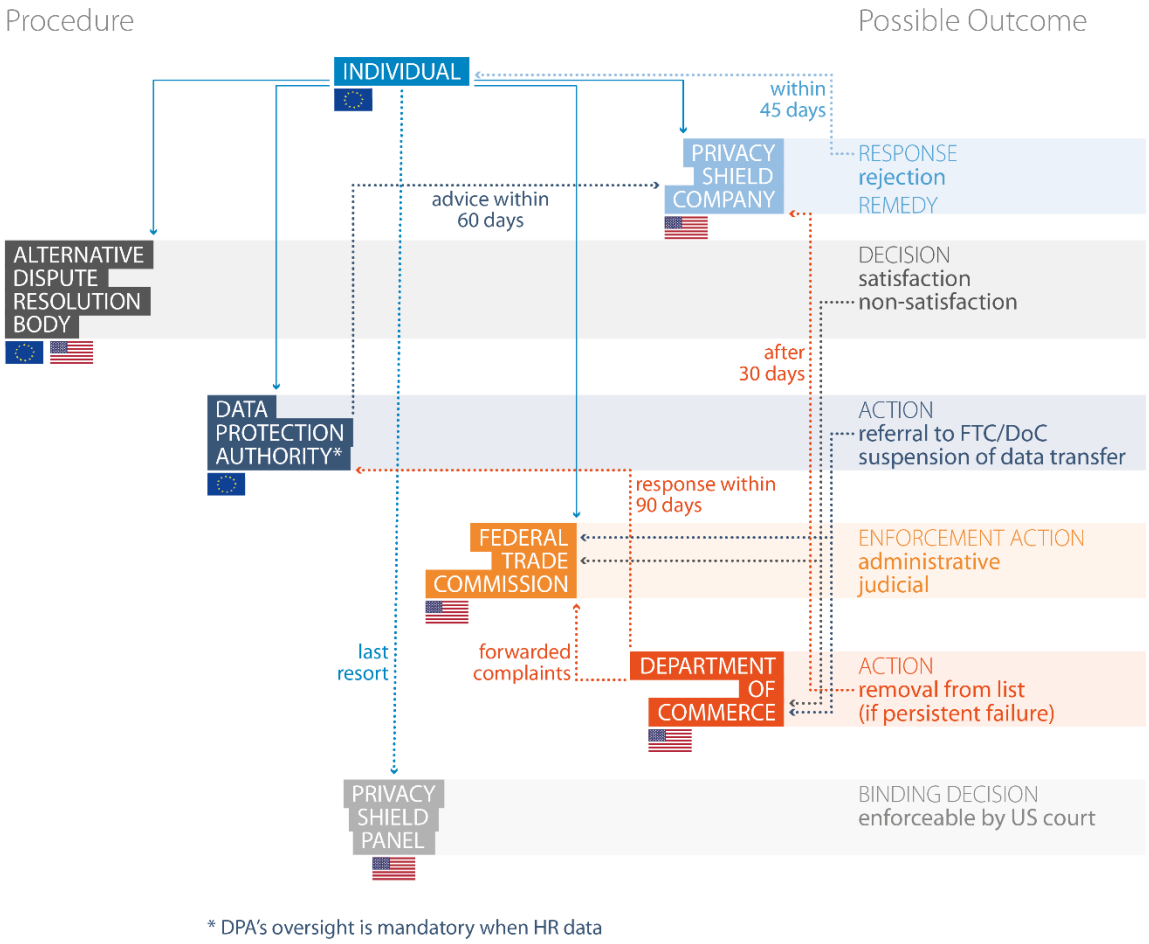
(5) The firms using PS are subject to US authority investigatory and enforcement powers, such as the FTC. Priority will be given to referral of non-compliance from independent dispute resolution bodies or self-regulatory bodies, DPAs and the DoC. Individuals will still be able to directly submit claims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

---

[88] 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).

[89] Section 5 FTC Act, 15 U.S. Code § 45 covering unfair and deceptive practices by companies.

Figure 1 – Redress mechanisms available to individuals



Source: EPRS, 2017.

(6) As a **last resort**, PS institutes a **Privacy Shield arbitration panel** if none of the above-mentioned avenues of recourse 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 up 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 (resourced with PS-using 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,[90] and breach of contract.

[90] 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.

3.3. The new US authorities' commitments and oversight mechanisms

3.3.1. 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 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.[91]

The DoC should 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 Privacy Shield;
(2) the review of organisations that need to be removed, either because they have not re-certified, have withdrawn, or are removed for persistent 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 action.

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.[92] 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 PS by a participating firm from DPAs.

3.3.2. 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) 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,[93] 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).[94] 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

[91] 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. 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.

[92] 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.

[93] Federal Trade Commission Act.

[94] See footnote 9.

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*,[95] action was taken against a US firm whose actions were directed at the United Kingdom market). However, at the time, 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 a misrepresentation complaint. Sometimes actions under section 5 involved violation abroad.[96] 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.[97] 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).[98] 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.[99]

3.3.3. 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 transferred. 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 concerns the US legal framework on data access by intelligence and other US authorities mentioned in the annexes to the PS.[100] As regards the issue of bulk collection of data, the EU Commissioner confirmed having received further assurance from US authorities that bulk collection of 'signals intelligence' (e.g., gathering of communication signals)[101] 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).[102] These assurances allowed the

95 *Best Priced Brands, LLC, et al.*

96 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.

97 For more information on the procedures refer to the FTC website.

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

99 See for example, the *Facebook* case and the *Myspace* case.

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

101 The Article29WP remarked in its opinion on the lack of definition of signals intelligence in any applicable text.

102 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

Commission to conclude that the data processing remains within the limit of necessity and proportionality, as requested by the CJEU.

Concerning the oversight[103] 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 4.1.2.).

Box 7 – Avenues of redress for undue access and use of data by US public authorities

In the case of avenues of redress for undue access and use of data by US public authorities for national security purposes, the following are the main avenues open to individuals[104] 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.[105] 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.[106]

(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'.[107] 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

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).

[103] 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 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).

[104] 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).

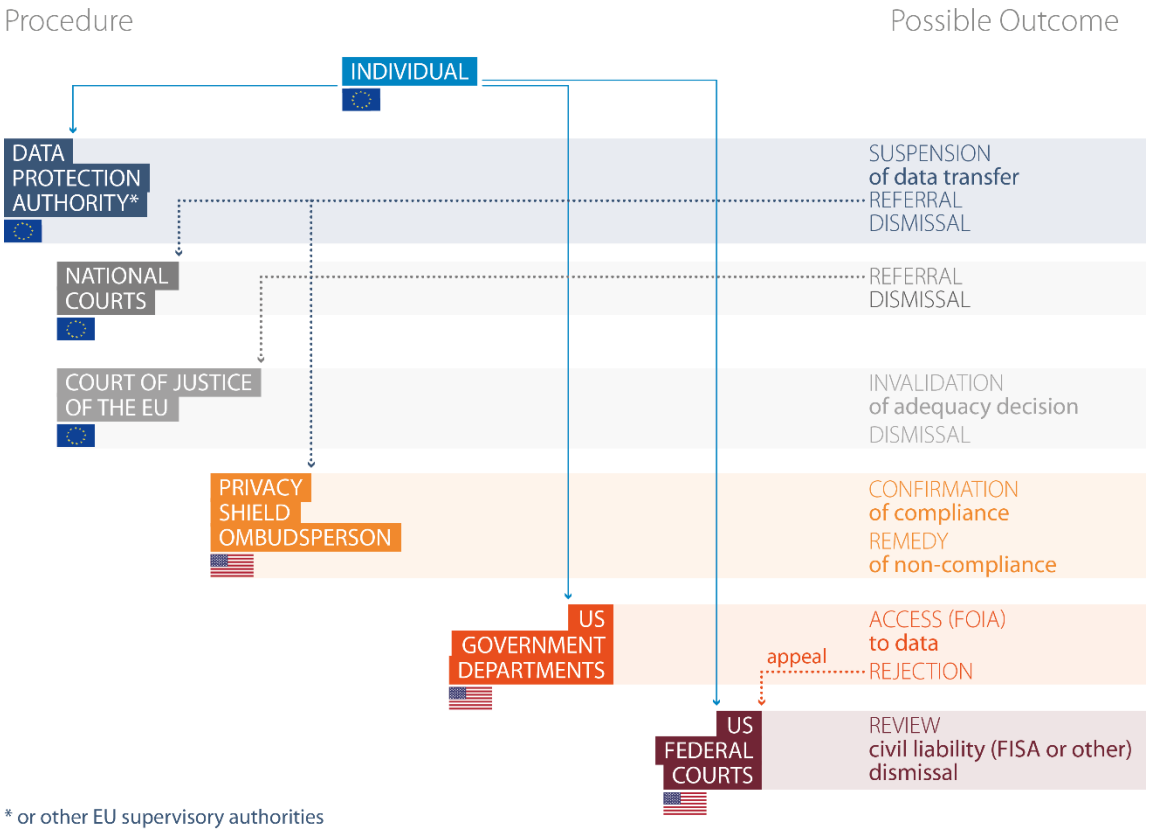
[105] 50 US Code § 1810 – civil liability.

[106] 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.

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

(existing) independent investigation structures such as the Inspectors-General[108] 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,[109] and has statutory public transparency requirements.

Figure 2 – Avenues of redress for undue access and use by US public authorities



Source: EPRS, 2017.

4. Towards a satisfactory and enduring tool?

4.1. Reactions to Privacy Shield

Different reactions have been registered in the aftermath of the adoption of the new arrangement. Most representatives of the commercial sectors in Europe and in the USA welcomed the new deal.[110] However, although formal adoption had been concluded, it was clear that it was not the end of the

[108] 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.

[109] Recommendations of the 9/11 Commission Act, Pub. L. 110-53, signed into law in August 2007 (codified in 42 USC §2000ee et seq.). An 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 and other materials, including classified information consistent with the law (annex VI p. 96).

[110] 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.

debate for many observers and policy-makers[111]. Nor did the arrangement seem to completely pacify the criticisms still present in the aftermath of publication of the new Privacy Shield (PS).[112] 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.

4.1.1. Privacy advocates

As to the **commercial aspects**, the PS is 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, as 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 'opt 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 stressed 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).[113]

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 of PS), 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, 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 Under-secretary 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

[111] 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.

[112] 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.

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

office would not guarantee the right to an effective remedy and a fair trial, as required by Article 47 CFR.[114]

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 US technology industry and government, and fails to provide an adequate level of protection.[115]

4.1.2. Article 29 Working Party and European Data Protection Supervisor

The **Article 29 Working Party issued a statement** on the amended Privacy Shield adequacy decision two weeks after its publication,[116] in which the Group of European DPAs welcomed the improvements of the final version, but expressed a number of concerns 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 issues 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, the EU DPAs expressed concern regarding the fact that **concrete assurances** to prevent this sort of surveillance could not be found in the PS.

In June 2017, the Art29 Working Party (WP29) sent a letter to Commissioner Jourová, in view of the preparation for the **first joint annual review**, which it deemed 'a fact-finding mission'. This annual review, which took place in September 2017 and in which WP29 also participated, was meant to assess the efficiency and robustness of the PS and to verify if the remaining issues have been solved (see below). Even before that, WP29 committed itself to proactively **assist data subjects** when dealing with complaints, and to provide suggestions to data controllers to comply with their obligations under the PS. Finally, the Article 29 WP appeared at that time willing to give the new PS a chance (backing Commissioner Jourová's claim), but took a **cautious approach**, rather than giving a true endorsement.

The importance given by commentators on the PS to the existence of oversight mechanisms and effective and agile redress systems was also shared by the **EDPS**, Giovanni Buttarelli,[117] who, regarding the 'likely longevity' of the Privacy Shield, claimed that 'we need a robust model for how

---

[114] Ibid. Max Schrems would still see difficulties in the 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'.

[115] BEUC, press release, 12 July 2016, 'Privacy Shield opens hole in protection of EU citizens' privacy',.

[116] See Article29WP statement on the Decision of the European Commission on the EU-US Privacy Shield. Moreover, the 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.

[117] 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.'

bilateral data sharing agreements can work…'. Buttarelli's hope is ultimately that, with the **GDPR** (fully in force from May 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' and also that a more robust instrument is needed in the long term.[118]

4.1.3. The European Parliament resolution of April 2017

Following a 2016 resolution on 'transatlantic data flow',[119] the EP adopted a resolution on the adequacy of the protection afforded by the EU-US Privacy Shield in April 2017, welcoming the Commission's efforts, but also expressing persisting concerns. Among other things, it called on the European Commission 'to seek clarification on the legal status of the "written assurances" provided by the US authorities and to ensure that any commitment or arrangement foreseen under the Privacy Shield is maintained following the taking up of office of a new administration in the United States'. Also it deplored the fact that the EU-US Privacy Shield does not explicitly prohibit the collection of bulk data for law enforcement purposes[120].

A new resolution on the same topic was adopted by the EP in July 2018 (see below).

4.2. Initial implementation and way forward

4.2.1. Initial Implementation

- Regarding the **attitudes of companies** (which may decide to stick to alternative tools), some scholars[121] 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; currently about 3 330 organisations have submitted certification.[122] This number is much smaller than the 4 000 companies that were registered under the Safe Harbour (SH). There could be a number of 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, and (3) the PS has a certain cost for firms adopting it.[123]

---

[118] *Ibid*.

[119] On that occasion, the EP, voicing concerns about 'deficiencies' in the (at that time) proposed new deal, urged the Commission to follow the indications of the EU national data protection authorities (Art29WP) regarding both the commercial aspects and the access by US public authorities to data transferred from the EU, such as 'the lack of specific rules on automated decisions and of a general right to object, the need for stricter guarantees on the independence and powers of the Ombudsperson mechanism, and the lack of concrete assurances of not conducting mass and indiscriminate collection of personal data (bulk collection)'. The EP also considered 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'.

[120] Other issues that the EP asked the Commission to address include: the fact that persisting concerns could lead to a new challenge to the adequacy decision being brought before the courts in the future, with consequences as regards both respect for fundamental rights and the necessary legal certainty for stakeholders; the lack of specific rules on *automated decision-making*, on a *general right to object*, and the lack of clear principles on how the Privacy Shield Principles *apply to processors* (agents); the need for a uniform definition of *bulk surveillance* linked to the European understanding of the term; the uncertain existence and quorum of the PCLOB, important for the oversight and transparency of U.S. measures; the need to clarify the impact of the Executive Order 12333 on remedies and the *right to judicial redress* for Europeans in the US. On the implications of similar executive orders, see E. Guild, D. Bigo & S. Carrera, Tramp's Travel Bans, Harvesting personal data and requiem for the EU-US Privacy Shield, CEPS Policy Insights No 2017/13 April 2017.

[121] See A. Mantelero, op. cit.

[122] See the list on PrivacyShield website.

[123] On this last point, the DoC has published the annual fees that an US institution must pay to the International Trade Administration administering the PS to cover the arbitral costs under the PS. Moreover the organisations have also additional direct costs as they must be able to provide readily available independent recourse mechanism to hear individual complaints at no cost to the individual.

- The FTC has started enforcing the Privacy Shield. Within the first year it had settled at least three cases of misrepresentation concerning three companies (*Decusoft, LLC; Tru Communication, Inc; Md7, LLC*). They claimed to be certified under the EU-US PS, but in reality they had failed to complete the certification process.[124] Those cases also have political meaning, as the FTC wants to underline its commitment to the PS framework.
- As for the challenges, the Privacy Shield could be brought in front of national and European **courts** by individuals (in so far as the applicant has an interest), European DPAs[125] or associations, with regard to its adequacy. Indeed, recourse has been made in 2016.[126] Also, limitations to provisions on general and indiscriminate data *retention by Member States* have been reiterated in Joined Cases C-203/15 and C-698/15 - *Tele2Sverige/ Watson*.[127] As for more recent challenges, a '**Schrems 2**' case is pending before the CJEU as the Irish High Court, after a decision taken in October 2017,[128] made reference in April 2018 to the CJEU with several questions on the effectiveness of remedies in US law for EU citizens whose data are transferred to US[129].
- While binding corporate rules and standard contractual clauses issued by the Commission remain **alternative tools** for data transfers, the legality of these tools is also being challenged in this latter case. The referral by the Irish High Court to the CJEU mentioned above and containing the questions on whether US law allows mass indiscriminate processing in breach of EU law, aims to determine the legal status of data transfers under Standard Clauses.

4.2.2. Review and outlook

(a) The first Annual review

The annual review, provided for in the Commission's adequacy decision in order to assess the efficiency and robustness of Privacy Shield, took place in the USA in September 2017 in Washington, DC.[130] Representatives of the European Commission, of the EP's LIBE committee, of the EDPS, and of the Art29WP participated in the review, considered as 'a fact-finding mission to obtain the relevant information and evidence on the robustness of the Privacy Shield'.[131]

After the first talks, Commissioner Jourová said that she had been reassured by US Secretary of Commerce Wilbur Ross that 'America first' does not mean 'America only'.[132] In October, the Commission released a **report** concluding that the PS has passed its first annual review and that the USA ensures an adequate level of protection for data transferred to participating companies in the

[124] See FTC press release 'Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework', 8 September 2017.

[125] The Hamburg DPA, for instance, seems willing to ask the CJEU to check the validity of the PS decision.

[126] As Reuters reported, a challenge against the Privacy Shield adequacy decision (T-670/16) was filed by the DRI against the European Commission in September 2016 but was dismissed by the Court in November 2017. An action for annulment has also been brought by La Quadrature du Net and Others (Case T-738/16).

[127] The principles emerging from this ruling, which confirms the consistent jurisprudence mentioned above on data protection, were also taken into account in another ruling, regarding this time the CJEU Opinion on the EU-Canada PNR agreement (which provides, though, for the sharing of data for law enforcement purposes). The Court held that the agreement had to be revised because not in line with the fundamental rights requirements of EU law. See synthesis in S. Monteleone, CJEU Opinion on EU-Canada PNR agreement, EPRS 'At a glance' note, September 2017.

[128] Irish High Court Decision, *Data Protection Commission v. Facebook and Schrems*, 3 October 2017.

[129] *Irish Times*, High Court sets out 11 questions for ECJ on EU-US data transfers, 12 April 2018.

[130] See Joint Press Statement from US Secretary of Commerce Ross and Commissioner Jourová on the EU-US Privacy Shield Review, 21 September 2017.

[131] Article 29 Data Protection Working Party Letter to the European Commission on the Privacy Shield Joint Review, 15 June 2017.

[132] C. Stupp, Jourova reassured 'America first' does not weigh on EU-US privacy shield, Euractiv, 19 September 2017.

USA.[133] On the basis of these findings, the report concludes that the US authorities have put in place structures and procedures to ensure the functioning of the PS, in particular new redress possibilities for Europeans. Still, while an acting Ombudsperson has been appointed, the nomination of the permanent Ombudsperson is still pending. The safeguards mentioned in the PS on the US side for personal data access by public authorities would remain in place, in particular Presidential Policy Directive 28 (PPD-28) on signals intelligence.[134] Meanwhile, Commissioner Jourová stressed the need for improvement in the implementation.[135] The report included a series of recommendations, such as: tougher monitoring of companies' compliance by the US Department of Commerce; appointment of a PS Ombudsperson to deal with Europeans' complaints concerning access to personal data by US authorities as well as appointment of the missing members of the Civil Liberty Oversight Board.[136]

Other concerns regard the follow-up of the controversial Section 702 of the Foreign Intelligence Surveillance Act (FISA) that allows agencies like the NSA to gather information on foreigners abroad; expired in January 2018, it was re-authorised by the US Congress for another six years at the beginning of 2018.[137]

(b) Article29 Working Party assessment following the annual review

The Article 29WP also presented its main findings of the joint review in its November 2017 report.[138] While welcoming the efforts made by US authorities – such as the prior checks of certified organisations, for the commercial aspects, and the increased transparency on the use of surveillance powers, for the access by public authorities to data transferred – the Article29WP also pointed out several **unresolved issues**.

Regarding commercial issues, it highlighted in particular: the lack of clear information on onward transfers and on available remedies for data subjects, calling for increased supervision of companies' compliance.[139] Major concerns related to the access by US authorities to data transferred under Privacy Shield in the law enforcement and security area.[140] Finally Article 29WP asked the Commission and US authorities to restart discussions and to set up an action plan for addressing the concerns with priority to be given (to the appointment of an independent Ombudsperson and the appointment of the PCLOB members. Article29WP warned of the possibility to bring the

---

[133] European Commission, Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–US Privacy Shield, 18 October 2017.

[134] On the relevance of preserving these instruments for the US economy, see C. Kerry & A. Raul, The Economic Case for Preserving PPD-28 and Privacy Shield, Lawfare Blog, 17 January 2017. For major US privacy laws, see M. Rotenberg (ed.), 'Privacy Law Sourcebook 2016: United States Law, International Law, and Recent Developments', EPIC 2016 (also taking into account the EU GDPR).

[135] European Commission Press Release, EU-US Privacy Shield: First review shows it works but implementation can be improved, 18 October 2017.

[136] *Ibid.*

[137] See US Congress, H.R. 4478: FISA Amendments Reauthorization Act of 2017. The House Judiciary Committee had approved in November 2017 a bill to reauthorize section 702. See in the news D. Volz, Trump signs bill renewing NSA's internet surveillance program, Reuters, 19 January 2018 and criticisms by, e.g., Electronic Frontier Foundation.

[138] Article 29 Working Party, EU-US Privacy Shield- First annual joint Review, 28 November 2017.

[139] Other recommendations in this area include: further improvements with regard to the handling of HR data, the rules on automated-decision making/profiling and self-certification process.

[140] In particular, the Article29WP called for binding commitments that data collection under section 702 FISA is not indiscriminate and access to data does not occur on a generalized basis: necessity and proportionality of targets under the section 702 should be assessed by the PCLOB (once fully installed) and the process of applying 'selectors' to be better clarified. Moreover, in case of re-authorization of section 702, it suggested improvements, such as precise targeting criteria.

Commission's adequacy decision on Privacy Shield to national courts in order for them to make a reference to the CJEU for a preliminary ruling.[141]

(c) Privacy Shield with regard to the new European legal framework

Although the PS already contains aspects not covered by the 1995 Data Protection Directive in order to be in line with the GDPR (such as onward transfers of data), a new assessment of the PS will have now to take into account that the **GDPR** is fully applicable,[142] in order to make, if required, the necessary improvements to the EU-US data transfer framework, with the GDPR as a legal basis.[143] One of the main changes of the GDPR as regards the 1995 Directive is its 'extended' territorial scope (Article 3) so that it has implications at a global level. It may, in fact, apply to any companies, EU-based or not (see box below).

The Commission published its guidelines on GDPR application in January 2018 and launched a practical online tool:[144] in the related communication, the Commission stressed that, while the architecture of the rules on international transfers in the GDPR remains essentially the same as that of the 1995 Directive, the reform clarifies and simplifies their use. WP29 has also issued Guidelines on Article 49 of the GDPR, i.e. on data transfer to third countries.[145]

GDPR: main changes

- *Scope*

- Like the 1995 directive, GDPR applies to data-processing activities of a *controller or a processor established in the Union*, regardless of whether the processing takes place in the EU or not; *and*
- it applies to the processing of personal data of individuals who are in the Union by a controller (or processor) not established in the Union in the case of *offering of goods or services to individuals in the Union* (for payment or not); or in the case of monitoring of individuals' behaviour (which takes place within the Union).
- Finally it applies to data processing by a controller not established in the Union by virtue of public international law.

- *Stronger safeguards for individuals' rights*

- According to the *accountability* principle, the data controller should be able to demonstrate his/her compliance with the rules;
- new rights are introduced, such as the freedom to transfer personal data from one service provider to another (*data portability*) or to have one's own data deleted when there are no legitimate grounds to retain them (*right to be forgotten*)[146].

- *Increased harmonisation and reduced administrative burden*

- The new rules are expected to be applied in a uniform manner across the EU, reducing fragmentation and legal uncertainty. The reform would minimise costs for businesses, by removing existing obligations, e.g. to notify all data processing to DPAs.

[141] The EDPB (replacing Art29WP) stated after its second plenary meeting in July 2018, in which the US Ombudsperson responsible for national security complaints under the PS took part, that the meeting did not provide a conclusive answer to the concerns raised by its predecessor (WP29) and that these issues will remain on top of the agenda during the Second Annual Review (planned for October 2018), calling for evidence from the US authorities in order to address these concerns.

[142] See EPRS 'At a Glance' note, GDPR goes live: A modern data protection law, 2018

[143] 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'. The GDPR will be complemented by the specific e-Privacy Regulation (in progress).

[144] European Commission, press release, Commission publishes guidance on upcoming new data protection rules, and communication 'Stronger protection, new opportunities', 24 January 2018.

[145] Article 29 Working Party, Guidelines on Article 49 of Regulation 2016/679, 12 February 2018.

[146] See EPRS compendium 'What is Europe doing for its citizens?', EP Open Days 2018, p. 17.

- a single data protection authority (DPA) would be responsible for a company operating in several countries, i.e. the DPA where the company has its main base ('one-stop-shop' system)

- *Simplified international transfers of data outside the EU*

- As general principle, data transfer to third countries can take place only if the controller is compliant with the GDPR, including for onward transfers.
- Transfers may take place (as in the 1995 directive) on the basis of a Commission adequacy decision, which means no specific authorisation is required; however this assessment should be based on strict criteria (e.g. existence of relevant legislation, respect for human rights; effective functioning of independent supervisory authorities; and international commitments).[147]
- Alternative tools include: a simplified process for BCR (subject to requirements), which implies that companies can adopt these rules voluntarily without the need to be verified by data protection authorities; a legally binding instrument between public authorities; standard data protection clauses approved by the Commission; an approved certification mechanism; contractual clauses between the controller and the recipient in the third country.

- *Stronger independent supervisory authorities and EDPB*

National authorities have their powers enhanced and they now convene at the EU level in the European Data Protection Board (EDPB) replacing Art29WP.

4.2.3. The Facebook/Cambridge Analytica scandal and the latest EP resolution

Taking into account the results of the joint annual review on the PS and the remaining issues, and also in view of the recent **revelations**[148] about the misuse of users' data by Facebook and Cambridge Analytica (which are certified companies under the Privacy Shield), in May 2018 the EP LIBE committee discussed a motion for a new EP resolution 'on the adequacy of the protection afforded by the EU-US Privacy Shield'.

The Facebook and Cambridge Analytica case

Around mid-March 2018, some newspapers reported that the UK-based political consulting firm, Cambridge Analytica – that had worked on Donald Trump's 2016 Presidential campaign – had, in 2014, improperly obtained information on 50 million (then shown to be 87 million) Facebook users (including 2.7 million Europeans), without their consent. According to whistleblower and former Cambridge Analytica employee, Christopher Wylie, the collection of data was initially made **via a third-party App** that 270 000 Facebook users had installed (for a psychology test). It seems that the latter was developed by a researcher in UK, who had obtained the permission of

[147] See Art 45 GDPR (transfers on the basis of an adequacy decision) stating that:

1. A transfer of personal data to a third country ... may take place where the *Commission has decided that* the third country ... *ensures an adequate level of protection*. Such a transfer shall not require any specific authorisation.

2. [...] the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, **including concerning public security, defence, national security** and criminal law and the access of public authorities to personal data, as well as the *implementation* of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country..., case-law, as well as...*effective* administrative and judicial redress for the data subjects [...];

(b)the existence and effective **functioning of one or more independent supervisory authorities** in the third country...,with responsibility for... enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the **international commitments** the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data." Art 46 states that in the absence of an adequacy decision, it is possible to transfer personal data to a third country ... only if the controller *has provided appropriate safeguards*, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available". Article 49 contains **derogations for specific situations** (public interest).

[148] See I. Lapowsky, 'Facebook Exposed 87 Million Users to Cambridge Analytica', Wired, 4 April, 2018.

these initial users for research purposes. Data of these users and of the friends of their friends were collected (exponentially) and passed to Cambridge Analytica, which used that data to target online voters/users with personalised political advertisements, thus manipulating their behaviour with the aim of helping Donald Trump win the US presidential election in 2016 (the same system is also said to have been used by pro-Brexit groups to influence UK voters in the referendum on EU membership). In 2014, Facebook announced it had made changes to restrict app developers' access to data.
In Europe, the revelations have raised criticisms and concerns. The **EP President**, Antonio TAJANI, released a statement on 19 March and confirmed the commitment of the EP to investigate fully on these allegations of misuse of data considered as 'an unacceptable violation of our citizens' privacy rights'. On 12 April, the EP decided to invite Facebook CEO Zuckerberg to explain himself to the EP. **Commissioner Jourová**, who is said to be unsatisfied by the explanations received from Facebook, promised to take all possible legal measures and stronger enforcement granted by the GDPR. In other words, if the violation had happened after the entry into application of the GDPR, the consequences for Facebook would have been much more serious; Facebook and other tech giant still need to comply with the new rules. A heated debate took place on these issues during the EP plenary session on 18 April 2018. Zuckerberg, praising the new EU data protection rules as the right ones (GDPR), declared that he intends to comply with it (e.g. on privacy settings). Also, the **WP29** issued a statement on 11 April 2018 in which Facebook's apologies are said to be not sufficient, and the establishment of a Social Media Working Group is announced. Also the **European Data Protection Supervisor** (Opinion 3/2018 on online manipulation and personal data, 19 March 2018) Giovanni Buttarelli affirmed that what had happened with Cambridge Analytica was not a mistake, but a symptom of a predominant business model, and thus relying on the goodwill of tech companies to regulate themselves is not enough. Finally, for some experts the really big change to come is around **enforcement**, because, while the EU has had long established data protection standards and rules, it had lacked the teeth to impose compliance. The teeth would come with the GDPR now fully in place.

The EP's (non-binding) **resolution** was adopted in plenary on **5 July 2018**, and it deems the Privacy Shield not adequate to protect individuals' rights.[149] It considers first the institutional aspects (i.e. the delay taken in the designation of the remaining members of the oversight bodies) as well as both commercial[150] and law-enforcement and security issues.[151] It also stresses that the assurance of effective redress to EU citizens would be void as long as a permanent, independent and empowered ombudsperson is not appointed (point 7).

Concerns were expressed by EP Members also in the wake of the recent revelations of data misuses, on the risks that the democratic process may suffer if data are used to manipulate political opinion or voting choices (given European elections are scheduled for June 2019).

While the EP welcomes the calls for the US legislator to move towards a general privacy act,[152] strong concerns raised in the resolution relate to the **CLOUD Act** (Clarifying lawful Overseas Use of Data), enacted by the US Congress in March 2018, which extends the abilities of US and foreign law

[149] EP resolution of 5 July 2018, Adequacy of the protection afforded by the EU-US Privacy Shield.

[150] In particular, it calls on the US authorities to undertake proactively *ex officio* reviews to monitor the effective compliance of companies with the PS in order to avoid false certification claims; to act upon revelations on Facebook /CA and if needed to remove such companies from the PS list.

[151] In particular, it notes that the orders made in the US under Sec. 702 FISA covering foreign intelligence targets have increased; calls for guarantees that data collection under Sec. 702 is not on a generalised basis (bulk collection); affirms that the reauthorisation of Sec. 702 questions the legality of the Privacy Shield; notes the persisting obstacles to judicial redress for non-US citizens subject to surveillance.

[152] Currently, only sectoral and state laws exist. Recent developments registered in legislation and case law in the privacy field include the **California Consumer Privacy** Act of 2018 and *Carpenter v. United States*.

enforcement authorities to access e-communications (emails and social media posts) held by private companies, like tech companies, and stored in servers outside the USA.[153] In this resolution, the EP deplores that the Commission and the US authorities did not set up any action plan in order to address the deficiencies identified by Art29WP, and concludes by calling on the Commission to suspend the Privacy Shield unless the US fully complies with it by 1 September 2018.[154]

The European Commissioner for Justice, Consumers and Gender Equality, Vera Jourová, from her side, sent a letter at the end of July to Wilbur Louis Ross Jr., the US Secretary of Commerce, criticising the US administration's failure to appoint a senior ombudsman (to oversee the Shield and to deal with EU citizens' complaints) and demanding that the US remedy the situation by October 2018. While Jourová was not ready to suspend the pact, she aims to make sure that the enforcement of the Shield is a priority for the US authorities[155].

The second joint annual review is planned for October, likely to take place in Brussels.

The possibility to suspend the data-exchange deal was provided for in Directive 95/46 and is set out now in the GDPR which states that if there is not adequate protection, data transfers should be suspended. EU data protection authorities are also called on to take enforcement actions and to suspend transfers when they are informed of non-compliant companies.

4.2.4. Privacy Shield and other countries

The impact of PS goes beyond EU-US relations alone and closely influences the relationship between the US and other countries.

- *(a) Application to the EEA countries*

- Because of the importance of data protection for the functioning of the internal market, EU data protection law has European Economic Area (**EEA**) relevance: in other words the EU framework also has to be implemented by EEA countries (Norway, Iceland and Liechtenstein). The EEA countries therefore had to incorporate the EU-US adequacy decision in EEA law. To that effect a Joint Committee decision was adopted on 7 July

[153] Two main aspects of the CLOUD Act stand out: first, the ability of the US government to compel tech companies to disclose the contents of communications stored in servers in foreign countries. To this end, the act amended the Stored Communications Act, as part of the Electronic Communications Privacy Act (ECPA), to compel companies to provide communications data in their control pursuant to warrants of US courts, *regardless* of whether data are stored inside or outside the USA. In a recent case, Microsoft refused to disclose contents of an email stored outside the USA (in Ireland) and the dispute, before the Supreme Court (in *United States v. Microsoft*), was declared resolved in April 2018 after Congress passed the CLOUD Act. As for the second aspect, the CLOUD Act authorises the US government branch to conclude international agreements through which selected countries can access data directly from US companies for prosecution of crimes. Before the Cloud Act, foreign countries were required to use mutual legal assistance or letters of rogatory mechanisms, and the related requests reviewed by US courts for authorisation. The act provides that data requests do not target US persons and requires that the foreign country has adequate law and procedures to protect civil liberties (to be assessed by the executive branch). While some observers praised it as a new form of cross-border data sharing, and a practical remedy to demands for evidence stored overseas in criminal cases, others criticise it for the risks it poses to civil liberties and rights by avoiding requirements previously necessary to obtain evidence. Congress can block (within 180 days) a proposed agreement from entering into force by enacting a joint resolution. See S. P. Mulligan, Cross-Border Data Sharing under the CLOUD Act, *CRS Report*, 23 April 2018 and Lexology.com 'Congress Passes CLOUD Act to Facilitate Law Enforcement Access to Overseas Data'.

[154] The EP's LIBE committee also started in June 2018 a series of hearings to better understand the impact of the Facebook/Cambridge Analytica case, after Mark Zuckerberg (Facebook's CEO) met the EP's President and the political group leaders in Brussels. Moreover, the Shield was also one of the topics discussed by a delegation of MEPs in a visit to Washington from 16 to 19 July 2018.

[155] Mehreen Khan, 'EU warns US over enforcement of Obama-era privacy deal', *Financial Times*, 30 July 2018

2017.[156] The EU-US Privacy Shield therefore also applies *ipso facto* to the three EEA countries.

(b) The adoption of a Swiss-US Privacy Shield

- The PS also had an impact on relations between the US and **Switzerland**. Switzerland is not part of the EEA and therefore the EU data protection law is not incorporated in the national framework as in the case of EEA countries.
- Switzerland therefore needed a specific adequacy decision to ensure continuity of data transfers with the EU. The adequacy decision between the EU and Switzerland recognises that the Swiss legal framework for data protection is essentially equivalent to that of the EU.[157] However, such a decision *inter alia* relies on the finding[158] that Swiss law also requires equivalent data protection for data transfers to non-signatory countries to Council of Europe Convention 108.[159] In light of this requirement, as well as the need to issue a partial adequacy decision for transfer of data to the US, Switzerland had concluded a Safe Harbour agreement with the US that was very similar to the EU agreement.[160]
- The CJEU judgement in the *Schrems case* had *per se* no legal effect on the Safe Harbour agreement between the US and Switzerland. However, the Federal Data Protection and Information Commissioner (FDPIC) considered that the reasons leading the CJEU to declare invalid the adequacy decision for the EU-US Safe Harbour, were equally valid for the US-Swiss Safe Harbour framework. Therefore, the latter framework was found to be insufficient to guarantee equivalent protection to that provided under Swiss law.[161] Moreover, FDPIC considered that it was particularly problematic to maintain the Safe Harbour system between the US and Switzerland while the EU had adopted a new framework (Privacy Shield) offering greater protection. Indeed such a situation could have led to triangular flows between the EU, Switzerland and the US that allowed circumvention of the stronger protection required under the privacy shield as illustrated by figure 3. That situation could have made the Swiss system inadequate to preserve the same level of protection as under EU law, thus leading to potential revocation of the EU adequacy decision. For that reason the Swiss Federal Council negotiated and concluded a Swiss-US Privacy Shield.[162]

Figure 3: The triangular flows issue with the old Switzerland-US 'Safe Harbour' agreement

[156] Decision of the EEA Joint Committee No 144/2017 of 7 July 2017 amending Annex XI (Electronic communication, audio-visual services and information society) to the EEA Agreement. One year later, another Joint Committee Decision was adopted to incorporate the GDPR into the EEA Agreement , including data transfer provisions: the EEA states have to amend their laws accordingly.

[157] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304).

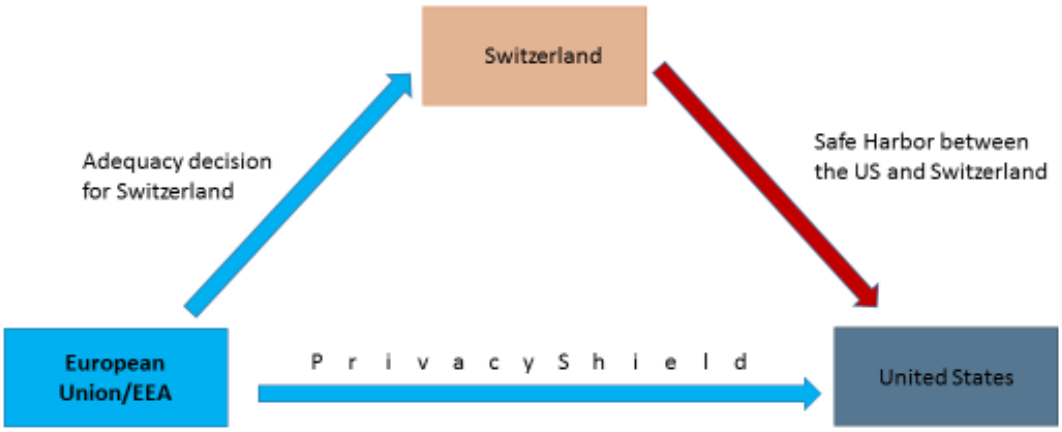
[158] Commission Staff Working Document: The application of Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland.

[159] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[160] Federal Data Protection and Information Commissioner press release: Switzerland and the US Conclude a Safe Harbor Agreement.

[161] Federal Data Protection and Information Commissioner press release: After the Safe-Harbor judgment: information on data transfers to the USA.

[162] Swiss-US Privacy Shield



Source: EPRS.

(c) Other considerations

- Another issue that needs further discussion, concerns the consequences of **'Brexit'**[163] on the PS and on triangular data flows between the USA, the United Kingdom (UK) and the EU. The PS will apply to the UK as long as it formally remains part of the EU. Once the UK exits the EU, cross-border data transfers to the UK would be similar to those with other third countries.[164]
- Moreover, if not directly, the PS may soon also be taken into account in relation to data transfers to **other third countries**.[165] On this point, the Commission published in 2017 a communication on Exchanging and Protecting Personal Data in a Globalised World, setting out its strategy for adequacy decisions on data transfers to third countries and also indicating alternative mechanisms. The Commission intensified dialogues with Japan aimed at the adoption of an adequacy decision on data protection framework.[166]
- There is also an ongoing discussion within the Commission on whether the assessment of third-country data protection should be done in 'adequacy decisions' as separate instruments (as is the case currently) or if they should be included in trade agreements.[167]
- Finally, third countries may also accede to Council of Europe Convention 108/1981, the only international legal instrument on data protection, recently amended.[168]

---

[163] The term *Brexit* refers to the withdrawal of the UK from the EU. See developments in EPRS 'At a glance' note by C. Cirlig, Framework for future EU-UK relations, March 2018.

[164] In this case, an adequate level of data protection should be ensured for companies to be able to make EU-UK data transfers. On Brexit and EU rules on data protection see European Commission, Notice to Stakeholders, 9 January 2018. However, there are several reasons to believe that the 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 not too difficult. See also C. Kuner, 'The global data protection implications of 'Brexit'', *International Data Privacy Law*, 2016, vol 6, No 3 and E. Ustaran, The future of international data transfers, *Privacy & Data Protection Journal*, 2018, Vol. 18, No 6.

[165] European Commission press release, Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers, Brussels, 10 January 2017.

[166] The EU and Japan concluded a deal on reciprocal adequacy of data protection systems in July 2018, which will be followed by a Commission adequacy decision in autumn. The EP's LIBE committee had visited Tokyo in November 2017 in view of its future assessment of the adequacy decision. Its focus was on the negotiations that the Commission had launched with Japan on data transfer in parallel to negotiations conducted on a trade deal with Japan (signed in July 2018). See also G. Greenleaf, 'Questioning 'adequacy' (Pt I) –Japan', *Privacy Laws & Business International Report*, (2017) 150, 1.

[167] POLITICO Brussels Playbook Breakfast with Věra Jourová, 18 October 2017.

[168] See CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and Protocol amending the Convention 108 of May 2018.

5. 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.

Bignami F. & Resta G., Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance in '*Community Interests Across International Law*' (E. Benvenisti & G. Nolte, eds., Oxford University Press, 2018) also available as GW Law Faculty Publications.

Boehm F., A comparison between US and EU data protection legislation for law enforcement purposes, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, September 2015.

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

Brkan M., Psychogiopoulou, E., *Courts, privacy and data protection in the digital environment*, Elgar, 2017.

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

EU Agency for Fundamental Rights, Report Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2017.

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).

Kaminski M. E. *Carpenter v. United States: Big Data is Different*, Response by, *Geo. Wash. L. Rev. on the Docket* 2 July 2018.

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

Mulligan S. P., Cross-Border Data Sharing under the CLOUD Act, *CRS Report*, 23 April 2018.

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

Voigt P., von dem Bussche A., *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer, 2017.

QA-07-17-018-EN-N

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 less than one year from the CJEU ruling, the Commission had adopted a new adequacy decision in which the new framework for EU-US data transfer, the *Privacy Shield* (2016), 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 paper. The first joint annual review took place in September 2017 on which both the Commission and Article 29 Working Party issued their own reports. Although progress is recognised, a number of concerns remain and new challenges to the Privacy Shield have arisen, among others, from the Facebook/Cambridge Analytica scandal, as pointed out by the European Parliament in its recent resolution.

This is a publication of the Members' Research Service]
EPRS | European Parliamentary Research Service

PDF ISBN 978-92-846-2234-4 | doi: 10.2861/675548 | QA-07-17-018-EN-N