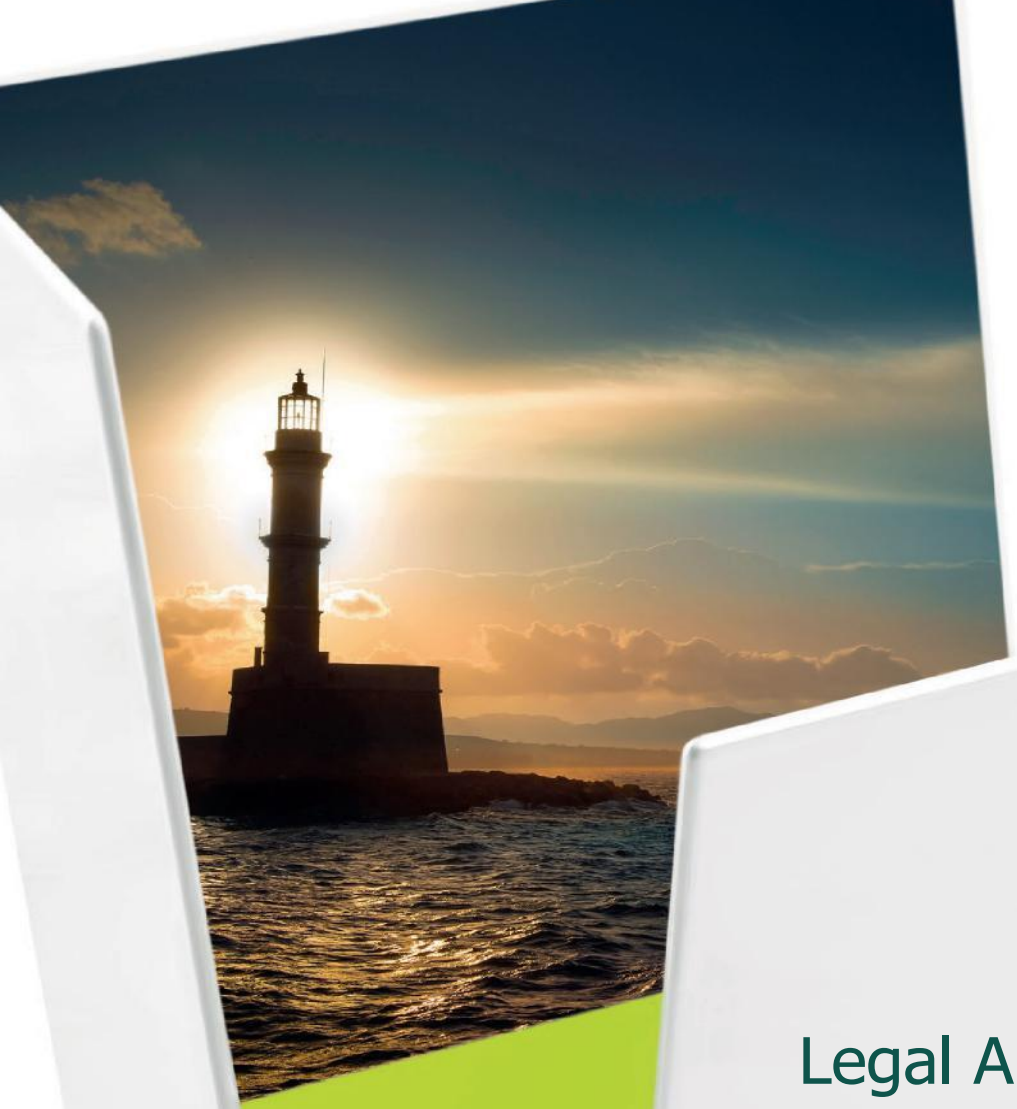

Legal Analysis of the EU-U.S. Privacy Shield

An adequacy assessment by reference to the jurisprudence of the Court of Justice of the European Union

Hogan Lovells

CONTENTS

1. INTRODUCTION – *IN SEARCH OF RIGOUR*

For decades, overcoming the limitations of European data protection law to transfer personal data to countries outside the European Union has been a compliance priority for organisations operating internationally. Global data flows are part of the fabric of modern communications and everyday commercial and social interactions. This is especially true of the transatlantic relations between the European Union and the United States. But in an increasingly digitalised and information-rich world, it can be cumbersome to put in place complex legal mechanisms aimed at legitimising international data transfers.

The original Safe Harbor framework was devised as a legal solution to a commercial challenge of political dimensions. It was widely embraced by multinationals across industry sectors and was frequently used as both a framework for global privacy law compliance and a tool for lawful data transfers by large corporations and small and medium-sized enterprises alike. However, its progressive demise, which culminated with a judgment from Europe's highest court invalidating its legal basis, led to an intense process of reform that concluded with the adoption of the EU-U.S. Privacy Shield.

The Privacy Shield has a crucial role to play in bridging the gap between European and American approaches to privacy and it is essential that it can be relied upon with complete legal certainty. Given the pressures to ensure that personal data transferred from the EU to the US is protected in accordance with European standards, the Privacy Shield will be subject to strict scrutiny by regulators and the courts as it becomes an established framework for compliance. Accordingly, assessing the robustness and legal validity of the Privacy Shield is a business and political necessity.

This report is aimed at providing an objective view on the adequacy of the Privacy Shield and follows a rigorous assessment of the framework based on European jurisprudence. We consider the historical background that preceded the adoption of the Privacy Shield and the precise legal test created by the Court of Justice of the European Union to determine its validity. Our conclusion – that the Privacy Shield Framework provides an 'essentially equivalent' level of protection for personal data transferred from the EU to the US – is based on our knowledge and understanding of European and US law and our interpretation of the fundamental legal principles that apply to the protection of privacy and personal data.

Eduardo Ustaran

Partner, London

Contributing authors:
Mark Brennan, Partner, Washington DC
Bret Cohen, Senior Associate, Washington DC
Victoria Hordern, Senior Associate, London
Katie McMullan, Associate, London
Ambassador Hugo Paemen, Brussels
Stefan Schuppert, Partner, Munich
Jonathan Stoel, Partner, Washington DC
Eduardo Ustaran, Partner, London
Nick Westbrook, Associate, London
Christopher Wolf, Partner, Washington DC

This assessment was commissioned by the Information Technology Industry Council and DIGITALEUROPE.

2. EXECUTIVE SUMMARY

This report is aimed at providing an objective view on the adequacy of the Privacy Shield and follows a rigorous assessment of the framework based on European jurisprudence. We consider the historical background that preceded the adoption of the Privacy Shield and the precise legal test created by the Court of Justice of the European Union ("**CJEU**") to determine its validity.

In particular, we consider the two key judgments from the CJEU examining respectively the Data Retention Directive and the Safe Harbor Decision in order to set out the criteria that the CJEU would likely use in the future to determine the validity of the Privacy Shield.

Taking all such jurisprudence into account, we consider that for the purposes of a valid adequacy determination by the Commission, the Privacy Shield must be able to meet the following specific criteria:

- Unrestricted and independent oversight by the EU data protection authorities ("**DPAs**") to examine a claim from an individual concerning the protection of his or her right to respect for private and family life and the right to the protection of personal data (Articles 7 and 8 of the Charter). This should be extensively interpreted, in the sense that such competence by the DPAs must have a practical application and be able to lead to the resolution of the matter.

- The Commission must also be entitled to periodically check whether the adequacy finding is still factually and legally justified.

- Any interference with Articles 7 and 8 of the Charter taking place in connection with the transfer of personal data to the US pursuant to the Privacy Shield must comply with Article 52 of the Charter so that:

  - It must be provided for by law, which should be validly enacted and enforceable.

  - It must respect the essence of the rights and freedoms recognised by the Charter, which is underpinned by the principles of democracy and the rule of law.

  - It must be proportionate so that the law must be appropriate to attain its legitimate objectives.

  - It must be limited to what is strictly necessary.

  - It must genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

  - The scope of the interference must be expressed in clear and precise rules.

  - There are minimum safeguards to ensure sufficient guarantees to protect the personal data against abuse and unlawful access and use.

  - There is proper accountability for third country public authorities accessing the data.

  - There are objective criteria determining the limits of access by public authorities to the data and its subsequent use for specific and strictly restricted purposes.

- Individuals must have a right to pursue effective legal remedies before an independent and impartial tribunal previously established by law, as enshrined in Article 47 of the Charter.

These are detailed and complex criteria that we have used as a firm benchmark for our assessment. In every instance, we have concluded that each criterion is met. In respect of some of the criteria, it is entirely beyond doubt that the Privacy Shield Framework meets the CJEU's objectives. With regard to any potential interference with fundamental rights, we consider that it is important to take into account the principles of democracy and rule of law which underpin the application of the US legal framework, as well as the specific circumstances and conditions under which US intelligence activities may lawfully take place. Of equal importance is the fact that the Privacy Shield Framework enables the exercise of various legal remedies, including before independent and impartial tribunals.

Ultimately, the Privacy Shield Framework differs significantly from the Safe Harbor Framework. The Privacy Shield Framework describes the rules governing access to data and therefore the extent of interference into fundamental rights and explains the safeguards to ensure effective protection of data against possible abuse and unlawful access. The Privacy Shield Principles should be read in conjunction with the assurances concerning limitations and safeguards under US law, so that it can be concluded that it is not the case that the fundamental rights of large numbers of individuals are likely to be infringed simply because their personal data is transferred under the Privacy Shield.

The considerable changes that have taken place in US domestic law since the Snowden revelations in June 2013 about surveillance practices underline the approach that the interferences with fundamental rights are necessary, proportionate and only as strictly necessary to attain the objectives of national security, law enforcement and the public interest.

In particular, the introduction of Presidential Policy Directive 28, the amendments to the US Foreign Intelligence Surveillance Act, the strengthened role of the US Foreign Intelligence Surveillance Court and other transparency requirements demonstrate the substantial political effort by the US government to strengthen privacy protections for all individuals. Furthermore, there is greater emphasis on targeted and tailored access by US agencies to data and, in particular, data collected in bulk can only be used for six specific national security purposes.

Whilst we accept that certain aspects of the Privacy Shield Framework would benefit from greater clarity, precision and accessibility, we are satisfied that these potential weaknesses do not affect the overall effect of the Privacy Shield Framework and the level of privacy and data protection that it affords. In reality the true level of data protection afforded by the Privacy Shield Framework will only be demonstrated by its functioning and the practices of its participants.

The key question this report sets out to answer is: ***Does the Privacy Shield Framework meet the criteria for adequacy under Article 25(6) of the Data Protection Directive as interpreted by the CJEU?*** Our assessment indicates that the Privacy Shield Framework does substantially meet the criteria laid out.

Therefore we conclude that, on the basis of our detailed assessment set out in this report, **the Privacy Shield Framework provides an 'essentially equivalent' level of protection for personal data transferred from the EU to the US.**

3. BACKGROUND AND RELEVANT EU LEGAL FRAMEWORK

3.1 Restrictions on transfers of personal data from the EU and adequacy findings

In 1995, the European Union ("**EU**") agreed to harmonise the differing approaches to data privacy protection in each of the individual Member States of the EU (the "**EU Member States**") and to establish a comprehensive EU-wide framework in the form of the EU Data Protection Directive 95/46/EC (the "**Data Protection Directive**").[1]

Article 25(1) of the Data Protection Directive placed a controversial requirement on the governments of EU Member States: to ban the transfer of personal data to any country outside the European Economic Area ("**EEA**") (which consists of the EU Member States together with Iceland, Liechtenstein and Norway) unless that third country ensures an adequate level of protection for the personal data in question.[2]

The Recitals of the Data Protection Directive do not explicitly explain the reason behind the prohibition on data transfers outside the EU. They recognise that cross-border flows of personal data are necessary for the expansion of international trade, but also state that the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited.[3]

In order to understand the basis for this regime, it is necessary to bear in mind the purpose of the Data Protection Directive as set out in Article 1: Member States must protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. In other words, the main aim of the legal regime established by the Data Protection Directive is to create a framework that protects and shields individuals' personal data from misuses and abuse.

However, such a framework would be very fragile if the protection afforded by it were to fall apart when personal data leaves the boundaries of the countries subject to EU data protection law. Therefore, the European institutions responsible for drafting and adopting the Data Protection Directive tried to preserve the effect of the new regime by blocking any attempts to weaken the protection afforded to individuals. In practice, this has created a situation that effectively requires the adoption of EU data protection standards by those outside the EU that wish to lawfully receive personal data originating in the EU.

3.2 Meaning of an 'adequate level of protection'

The general rule under Article 25 of the Data Protection Directive is subject to a case-by-case assessment of the adequacy of the level of protection afforded by the third country in question. This can be assessed by individual Member States or by the European Commission ("**Commission**"). In particular, the Commission has the power to make determinations of adequacy that are binding on the EU Member States, as considered in section 4 below.

According to Article 25(2) of the Data Protection Directive, such decisions of adequacy must be assessed in light of all the circumstances surrounding the data transfer. In addition, as part of that assessment, particular consideration must be given to:

---

1 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 the Free Movement of Such Data.

2 *'The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection'* Article 25(1) of the Data Protection Directive.

3 See Recitals 56-57 of the Data Protection Directive.

(a) the nature of the data;

(b) the purpose and duration of the proposed processing operation or operations;

(c) the country of origin and country of final destination;

(d) the rules of law, both general and sectorial, in force in the third country; and

(e) The professional rules and security measures which are complied with in that country.

The Article 29 Working Party, which is comprised of representatives of the national data protection authorities ("**DPAs**") of each of the EU Member States, the European Data Protection Supervisor and the Commission, (collectively "**Article 29 Working Party**") issued detailed guidance in July 1998 (notably, before the deadline for implementation of the Data Protection Directive) which sets out the core criteria that the Article 29 Working Party considers third countries should fulfil to provide an adequate level of protection for personal data.[4]

Following the Article 29 Working Party's advice, an assessment of the level of protection must comprise two basic elements: (a) the content of the rules applicable; and (b) the means for ensuring their effective application. Accordingly, the Article 29 Working Party identified a set of content principles and a basic enforcement mechanism, which can be regarded as the minimum requirements for the protection to be considered adequate.[5]

The content principles include:

(a) The purpose limitation principle*:* data must be processed for a specific purpose and subsequently used or further communicated only in so far as this is not incompatible with the purpose of the transfer.

(b) The data quality and proportionality principle*:* data must be accurate and, where necessary, kept up to date. The data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

(c) The transparency principle*:* individuals must be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and any other information that is necessary to ensure fairness.

(d) The security principle*:* technical and organisational security measures must be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

(e) The rights of access, rectification and opposition*:* individuals must have a right to obtain a copy of all data relating to them, and a right to rectification of such data where they are shown to be inaccurate. In certain situations, individuals must also be able to object to the processing of their personal data.

(f) Restrictions on onward transfers*:* further transfers of the personal data by the recipient of the original data transfer must only be permitted where the second

---

4 Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP12). Adopted by the Article 29 Working Party on 24 July 1998.

5 Ibid, pages 4 - 7.

recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection.

(g) Sensitive data*:* where 'sensitive' categories of data are involved, additional safeguards should be in place, such as a requirement that individuals give their explicit consent for the processing.

(h) Direct marketing*:* where data is transferred for the purposes of direct marketing, individuals should be able to 'opt-out' from having their data used for such purposes at any stage.

(i) Automated individual decision-making*:* where the purpose of the transfer is to make an automated decision in the sense of Article 15 of the Data Protection Directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

The enforcement mechanism required need not be based on a supervisory authority model, as is typically the case within EU Member States. What the Article 29 Working Party is concerned about is a system that meets the underlying objectives of a procedural system of data protection, namely:

(a) The delivery of a good level of compliance with the rules*:* a good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among individuals of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for the rules, as can systems of direct verification by authorities, auditors or independent data protection officials.

(b) The provision of support and help to individuals in the exercise of their rights*:* individuals must be able to enforce their rights rapidly and effectively, and without prohibitive cost, which means that there must be some sort of institutional mechanism allowing independent investigation of complaints.

(c) The availability of appropriate redress to the injured party where rules are not complied with*:* this is a key element, which must involve a system of independent adjudication or arbitration that allows compensation to be paid and sanctions imposed where appropriate.

Although the concept of an 'adequate level of protection' was established by the Data Protection Directive, it is worth noting that the same principle will be present in the forthcoming EU General Data Protection Regulation ("**GDPR**"), which was agreed by the EU's legislative institutions in December 2015 and is set to replace the regime created by the Data Protection Directive in 2018. Therefore, although our analysis focuses on the current state of the law and its judicial interpretation, our findings will be equally relevant in the context of the future legal framework under the GDPR.

3.3 Origins of Safe Harbor

Countries such as the US that approach the regulation of personal data privacy from a different perspective than countries in Europe, face certain challenges when trying to demonstrate an adequate level of protection according to the European standard. In the US, respect for privacy vis-à-vis government actors is broadly enshrined in the Constitution, and there are a number of statutory protections at a federal and state level directed at specific sectors or particular concerns (e.g. children's online privacy; health

data privacy), but there is no single European-style comprehensive privacy law that applies to all personal data. In order to bridge the different legal approaches and considering the large volume of data transfers carried out between the EU and the United States, the US Department of Commerce ("**DoC**") and the Commission devoted more than two years following the passage of the Data Protection Directive to develop a self-regulatory framework that would allow organisations to satisfy the requirements of the Data Protection Directive.

On 26 July 2000, following extensive negotiations, the Commission finally issued a Decision[6] ("**Safe Harbor Decision**") stating that the Safe Harbor Privacy Principles as issued by the DoC ("**Safe Harbor Privacy Principles"**) provided adequate protection for personal data transferred from the EU. This decision enabled EU personal data to be transferred to US-based companies that agreed to abide by the Safe Harbor Privacy Principles.

3.4 Safe Harbor Framework

The decision by US-based organisations to abide by the Safe Harbor Privacy Principles was entirely voluntary. Participation was open to any organisation subject to regulation by the Federal Trade Commission ("**FTC**"), which enforces a variety of consumer protection laws (including those related to unfair and deceptive practices), and to United States air carriers and ticket agents that are subject to regulation by the Department of Transportation ("**DoT**"). Financial firms and telecommunications carriers which did not fall under the jurisdiction of the FTC or the DoT for unfair and deceptive practices were not eligible to participate.

Organisations that decided to participate in the scheme had to comply with the relevant requirements (summarised below) and publicly declare that they did so. The organisation had to self-certify annually to the DoC in writing that it agreed to adhere to the Safe Harbor Privacy Principles. It also had to state in its published privacy policy statement that it adhered to the principles.

The requirements established by the Safe Harbor Privacy Principles were as follows:

(a) Notice: an organisation must inform individuals of the purposes for which it collects and uses personal information, how it can be contacted, to whom it intends to disclose the information and the choices and means available to individuals for limiting the use and disclosure of that information. This notice must be made available in clear and conspicuous language before the organisation uses or discloses the information.

(b) Choice: an organisation must offer individuals the opportunity to opt out of uses or disclosures involving their personal information, where such uses or disclosures are incompatible with the purposes for which the information was originally collected or subsequently authorised by the individual. With regard to sensitive personal information (i.e. data specifying the medical or health condition, the racial or ethnic origin, the political opinions or trade union membership, the religious or philosophical beliefs or the sex life of an individual) affirmative or explicit consent – opt-in – must be obtained if the information is to be used for a purpose other than that for which it was originally collected or subsequently authorised by the individual.

(c) Onward transfer: an organisation may only disclose personal information to third parties that (a) subscribe to the Safe Harbor Privacy Principles; (b) are subject to

[6] "Commission Decision of 26 July 2000 pursuant to Data Protection Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce".

the Data Protection Directive; or (c) enter into a written agreement whereby they undertake to provide at least the same level of privacy protection provided by the Safe Harbor Privacy Principles.

(d) Security: organisations processing personal information must take reasonable security measures and precautions to avoid its loss, misuse and unauthorised access, disclosure, alteration or destruction.

(e) Data integrity: an organisation may only process information relevant to the purposes for which it has been gathered. In addition, steps must be taken to ensure that the data are (a) relevant for the intended use; and (b) accurate, complete and current.

(f) Access: individuals must have access to personal information about them held by an organisation and be able to correct it, except where the burden or expense of providing access is disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

(g) Enforcement: organisations must abide by certain mechanisms of compliance with the Safe Harbor Privacy Principles, which provide recourse for individuals and consequences for non-compliance. At the very least, such mechanisms must include: (a) a readily available and affordable independent recourse mechanism to investigate and resolve individuals' complaints and disputes by reference to the Safe Harbor Privacy Principles and award damages where applicable; (b) a follow up procedure to verify the implementation of privacy practices; and (c) an obligation to remedy problems arising out of failures to comply with the Safe Harbor Privacy Principles.

3.5 Practical operation of the Safe Harbor Framework

Enforcement of the Safe Harbor Privacy Principles took place in the United States in accordance with US law and was carried out primarily under a private sector third-party independent recourse mechanism. This private sector self-regulation and enforcement mechanism was to be backed up as needed by government enforcement of federal statutes regulating unfair and deceptive practices, with an organisation's failure to comply with the Safe Harbor Privacy Principles (despite publication of the organisation's compliance) considered to be an unfair or deceptive practice.

Since its adoption, the Safe Harbor Framework has been fraught with challenges. Although the data protection requirements set out in the Safe Harbor Privacy Principles were meant to match the adequacy standards of the Data Protection Directive, its self-certification nature and the non-European style of its provisions attracted much criticism over the years. Perceived weaknesses included that participants did not perform required annual compliance checks and the lack of active enforcement by the FTC compared to other domestic cases. These factors led some EU DPAs to question the validity of the Safe Harbor Framework as an adequacy mechanism.

In March 2012, the EU and US issued a joint statement on data protection affirming that both were '*dedicated to the operation of the Safe Harbor Framework – as well as to our continued cooperation with the Commission to address issues as they arise – as a means to allow companies to transfer data from the EU to the United States, and as a tool to promote transatlantic trade and economic growth*'.[7] However, just over a year later in July 2013 and following the Snowden revelations in early June 2013, the then Vice-President of the Commission, Viviane Reding, stated at the Justice Council in Vilnius that '*the Safe*

[7] European Commission Memo/12/192, 19 March 2012.

Harbor agreement may not be so safe after all. It could be a loophole for data transfers because it allows data transfers from EU to US companies – although US data protection standards are lower than our European ones'. She also announced that the Commission was working '*on a solid assessment of the Safe Harbor Agreement*' which would be presented before the end of that year.[8]

3.6 European Commission's reaction to Snowden revelations

The revelations triggered by Edward Snowden in June 2013 about the mass surveillance operations carried out by the US National Security Agency ("**NSA**") had a very visible knock-on effect on the way in which the EU regulates international transfers of personal data. In light of the existing criticisms of the Safe Harbor Framework and amid allegations that companies that participated in the scheme might have been involved in US surveillance activities, calls for the revocation of the Safe Harbor Framework from activists and some of the DPAs led the European Parliament to adopt a resolution seeking its immediate suspension.[9] The Commission rejected doing so because of concerns that suspending the Safe Harbor Framework would adversely affect EU business interests and the transatlantic economy. However, it agreed that there were a number of weaknesses in the Safe Harbor Framework and had no choice but to reopen the dialogue with the US government to find a way of strengthening the framework and restoring its credibility.

The Commission announced this renegotiation on 27 November 2013 through two communications to the European Parliament and the Council of the EU ("**Council**"), entitled 'On the functioning of the Safe Harbor from the Perspective of EU citizens and Companies Established in the EU'[10] and 'Rebuilding Trust in EU-US data flows'[11] (together the "**Communications**"). In the Communications, the Commission stressed that the EU and US were strategic partners and that transatlantic data flows were critical to commerce, law enforcement and national security on both sides of the Atlantic. However, it also recognised that the Snowden revelations had damaged the EU's trust in this partnership, and that this trust needed to be rebuilt.

3.7 European Commission's concerns over Safe Harbor

In the Communications, the Commission noted that the Safe Harbor Framework had become a crucial part of the commercial partnership between the EU and US, with more than 3,000 companies signed up. However, the scheme needed to be reviewed in light of both the Snowden revelations and the massive increase in scale and importance of transatlantic data flows since the scheme was introduced.

The Commission pointed out that the majority of US internet companies reportedly directly affected by US surveillance programmes were members of the Safe Harbor scheme. This brought into question the level of protection afforded by the Safe Harbor Framework . In the Commission's words:

'*the personal data of EU citizens sent to the US under the Safe Harbor may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US.*'[12]

---

8 European Commission Memo/13/710, 19 July 2013.

9 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 (2013/2682(RSP).

10 "On the functioning of the Safe Harbor from the Perspective of EU citizens and Companies Established in the EU" COM(2013) 847 final, 27 November 2013.

11 "Rebuilding Trust in EU-US data flows" COM(2013) 846 final, 27 November 2013.

12 Ibid, page 4.

The Safe Harbor Framework contained an exception which permits disclosure of data transferred under the scheme to third parties "*to the extent necessary*" to meet national security requirements. The Commission called this exception into question, pointing out that '*large scale access by intelligence agencies to data transferred to the US in the context of commercial transactions*', as was reported by Snowden, was not foreseen when the Safe Harbor Privacy Principles were created.[13] Moreover, it questioned whether this access was in fact *'necessary and proportionate'* to national security interests, pointing out in particular that '*under these programmes, EU citizens do not enjoy the same rights and procedural safeguards as Americans*'.[14]

The Commission was also specifically concerned that the reported US surveillance programmes risked undermining the confidentiality of electronic communications[15], and indeed stated bluntly that '*Mass surveillance of private communication, be it of citizens, enterprises or political leaders, is unacceptable*'.[16]

In addition to concerns arising from the Snowden revelations, the Commission took the opportunity to address long-standing concerns within the EU about the perceived lack of enforcement by US authorities of the Safe Harbor Privacy Principles. The Commission argued that as a result, some Safe Harbor certified organisations were not in practice properly incentivised to comply with their obligations. In particular, a substantial number of Safe Harbor organisations had not made their privacy policies public, which itself made oversight and enforcement more difficult. It also noted that approximately 10% of US companies claiming to be Safe Harbor certified were not in fact listed as current members by the DoC, undermining the scheme's credibility.[17] The Commission argued that until these and other deficiencies were corrected, US Safe Harbor certified companies would have a competitive advantage over EU companies and the fundamental right to data protection of EU citizens would be negatively affected.

On a more practical note, the Commission also highlighted that the DPAs had the power (under Article 3 of the Safe Harbor Decision) to suspend data flows to Safe Harbor certified companies in certain situations.[18] This was already being considered by authorities in Germany. It noted the desirability of avoiding a 'difference in coverage', whereby the Safe Harbor Framework could only be used to transfer data to the US from certain EU Member States.

3.8 Renegotiation of Safe Harbor

In the Communications the Commission set out thirteen recommendations aimed at addressing the above identified weaknesses and ensuring that the Safe Harbor Framework remained an effective mechanism for facilitating commercial transatlantic data flows.[19] These recommendations focused on four broad priorities, as follows:

(a) Transparency

(i) Scheme members' privacy policies should be published on their websites

---

13 COM(2013) 847 final, page 16.
14 COM(2013) 846 final, page 4.
15 COM(2013) 847 final, page 16.
16 COM (2013) 846 final, page 2.
17 COM(2013) 847 final, pages 6-7.
18 Specifically, data transfers can be suspended by a national authority where: there is a substantial likelihood that the Safe Harbor Privacy Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authority in the Member State has made reasonable efforts to provide the company with notice and an opportunity to respond.
19 COM(2013) 847 final, page 17 onwards.

in clear and conspicuous language.

(ii) Scheme members' privacy policies should link to a list of all current members of the scheme maintained on the DoC website.

(iii) Scheme members should disclose the data protection provisions of contracts with any third party providers who processed data transferred to the US under the scheme.

(iv) The DoC should clearly identify companies which are no longer members of the scheme on its website. Those which cease to be members should still protect data received under Safe Harbor.

(b) Redress

(i) Scheme members' privacy policies should contain a link to a web page for the alternative dispute resolution ("**ADR**") provider serving as the members' independent recourse mechanism.

(ii) ADR should be readily available and affordable to individuals.

(iii) The DoC should monitor more systematically the transparency and accessibility of information ADR providers set out regarding how they deal with complaints.

(c) Enforcement

(i) A certain percentage of companies certifying or recertifying under Safe Harbor should be subject to ex-officio investigations to determine whether they are complying with their privacy policies.

(ii) Any finding of non-compliance should result in a follow-up investigation after one year.

(iii) EU data protection authorities should be informed where there are doubts about a company's compliance or a pending complaint.

(iv) False claims of Safe Harbor adherence should continue to be investigated.

(d) Access by US authorities

(i) Scheme members' privacy policies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbor scheme. Companies should be encouraged to indicate when they apply exceptions to the Safe Harbor Privacy Principles in order to meet national security, public interest or law enforcement requirements.

(ii) The national security exception should be used only when strictly necessary or proportionate.

The Commission recognised that achieving the last of these recommendations would require action on the part of US authorities, namely:

(a) reviewing whether US legal standards relating to US surveillance programmes which treat US and EU citizens differently are necessary and proportionate;

(b) providing more transparency around the legal framework of US intelligence collection programmes and their interpretation by US courts;

(c) providing more transparency around the scale of current US collection programmes; and

(d) improving oversight over US intelligence collection programmes by strengthening the role of the US Foreign Intelligence Surveillance Court ("**FISC**") – a federal court that oversees government requests for surveillance warrants for national security and foreign intelligence purposes – and introducing remedies for individuals.

On the basis of these recommendations, the Commission began discussions with US authorities aimed at updating the Safe Harbor Framework in January 2014.[20] The original aim was to identify remedies by Summer 2014 and implement them as soon as possible thereafter.[21]

In June 2014, Viviane Reding provided an update on the negotiations, reporting that the DoC had agreed to 12 of the Commission's 13 recommendations.[22] However, the sticking point was the final recommendation that the national security exception was only to be applied when strictly necessary and proportionate. Reding characterised the disagreement as "*a problem of definition … [The national security exception] should be an exception not a hoover. This must be clarified before we can give our agreement to [an updated] Safe Harbor*".

3.9 CJEU ruling on Maximillian Schrems v Data Protection Commissioner (Case C-362/14) ("*Schrems*")

Austrian law student Maximillian Schrems lodged a complaint with the Irish Data Protection Commissioner ("**Irish Commissioner**") in June 2013 requesting the termination of any transfers of personal data by Facebook Ireland to the United States. Mr Schrems claimed that Facebook Ireland – the data controller for Facebook's European users' data – could no longer rely on the Safe Harbor Framework to legitimise the transfers of his data to the US because of the wide access that US intelligence agencies had to such data as revealed by Snowden.

However, the Irish Commissioner rejected the complaint on the basis that the adequacy of Safe Harbor had already been determined by the Commission and therefore, it was not open to the Irish Commissioner to challenge the Commission's 'adequacy finding'. This was not accepted by Mr Schrems who remained adamant that the Safe Harbor Framework did not provide an adequate level of protection for his data. Therefore, Mr Schrems took the unprecedented step of seeking judicial review of the Irish Commissioner's decision.

Throughout the EU, the decisions of the DPAs may be challenged in court. In the case of the Irish Commissioner, the High Court of Ireland ("**Irish High Court**") is the competent tribunal for these purposes and the forum where Mr Schrems sought relief by requesting that the Irish Commissioner's rejection be overturned. The Irish High Court took the view that the main issue at stake was a matter of EU law. The Irish High Court explained that whilst the Irish Commissioner was indeed able to direct an entity to suspend data flows to

---

20 "Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Data Protection Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14, COM(2015) 566 final, page 3.

21 COM(2013) 846 final, page 7.

22 European Commission press release Speech 14-431, 6 June 2014.

a third country declared adequate by the Commission, this was only in circumstances where – unlike in this case – the complaint was directed to the conduct of that entity.

Therefore, the Irish High Court considered that what needed to be determined was whether the Irish Commissioner was absolutely bound by the Safe Harbor Decision, a question which is fundamentally a matter of EU law. In other words, the Irish High Court considered that Mr Schrems' real objection concerned not the conduct of Facebook Ireland as such, but the fact that the European Commission had determined that the Safe Harbor Framework provided adequate protection for data exported from the EU in the light of the disclosures made by Snowden regarding access to EU citizens' data by the US authorities. Since this is a matter of interpretation of the EU data protection legal framework, the Irish High Court referred this particular point for decision by the Court of Justice of the European Union ("**CJEU**") the highest judicial authority on the interpretation of EU law.

The CJEU held its first and only public hearing of this case on 24 March 2015. Mr Schrems' main argument was that the Safe Harbor Decision should be declared invalid because of its incompatibility with both the Data Protection Directive and the Charter of Fundamental Rights of the EU ("**Charter**"). Mr Schrems made a comparison with the CJEU's own decision in the *Digital Rights Ireland* case (see analysis in section 5.1 below) on the EU Data Retention Directive 2006/24/EC ("**Data Retention Directive**") and argued that the interference caused by the interception and surveillance of European citizens' data under the Safe Harbor Framework was even more serious. For this reason, Mr Schrems urged the CJEU to question the validity of the Safe Harbor Decision as a whole, even though the specific questions referred by the Irish High Court did not formally concern such validity.

Mr Schrems went on to argue that at the very least the Irish Commissioner had the overriding duty to protect his fundamental right to privacy and that the Commissioner's competence to render a decision on his question must be interpreted in light of this objective. Furthermore, Mr Schrems argued that it would be contrary to the independence of DPAs if those authorities were absolutely bound by the Commission's adequacy decisions.

On 6 October 2015, the CJEU issued its judgment[23] and declared the Safe Harbor Decision invalid. In its ruling, the CJEU also confirmed that a national EU DPA is always empowered to challenge the adequacy of data transfers and only the CJEU can invalidate a Commission's decision of adequacy.

3.10 Status of personal data transfers to the US

The CJEU's decision invalidating the Safe Harbor Decision has had the following consequences in practice:

(a) Transfers of personal data from the EU to the US previously covered by the Safe Harbor Decision are unlawful unless they are suitably authorised by DPAs or fit within one of the legal exemptions (mentioned in (b) below).

(b) Multinationals that relied on the Safe Harbor Decision as an intra-group compliance tool to legitimise data transfers from EU subsidiaries to their US parent company or other US-based entities within their corporate group need to implement an alternative mechanism such as the Commission's Standard Contractual Clauses (**"SCC"**) or Binding Corporate Rules (**"BCR"**) or ensure that

[23] *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, CJEU, Case C-362/14.

the transfer fits within one of the exemptions contained in Article 26(1) of the Data Protection Directive.[24]

(c) US-based service providers certified under the Safe Harbor Framework to receive data from European customers need to provide alternative guarantees for those customers to be able to engage their services lawfully.

It is also critical to appreciate that the CJEU did not rule on whether the Safe Harbor Privacy Principles were sufficiently close to the European data protection standards. In essence, the CJEU ruled that the Safe Harbor Decision was no longer a valid mechanism to legitimise data transfers because the Commission had not ensured that the Safe Harbor Decision addressed the potentially excessive interference of US law with the fundamental rights to privacy and data protection that exist under EU law.

This means that aside from the thirteen recommendations set out by the Commission in its Communications of November 2013 (as described in section 3.8 above and further examined in Appendix II below), the crucial aspect of *Schrems* from a future 'adequacy finding' perspective is the way in which the US legal framework is able to meet the specific criteria identified by the CJEU.

3.11 EU–U.S. Privacy Shield

On 29 February 2016, and after more than two years of negotiations with the DoC, the Commission released its much-awaited draft decision on the adequacy of the new EU–U.S. Privacy Shield framework, accompanied by information on how the framework will work in practice ("**Privacy Shield Framework**").

The Privacy Shield Framework's documentation is significantly more detailed than that associated with its predecessor, the Safe Harbor Framework, imposing more specific and exacting measures on organisations wishing to join the framework (as described in section 6.1 and Appendix III below). It also includes additional checks and balances designed to make sure that the privacy rights of EU individuals can be exercised when their data is being processed in the United States, as well as various official letters from US government officials providing assurances regarding the legal limitations affecting access to personal data by US government agencies. That said, the seven Privacy Shield Principles are largely aligned with the privacy practices followed by Safe Harbor certified organisations.

In relation to the Privacy Shield Framework, the Article 29 Working Party issued a preliminary statement on 3 February 2016 (before the relevant documentation had been publicly disclosed) welcoming the conclusion of the negotiations between the EU and the US on the introduction of the Privacy Shield Framework.[25] In this statement, the Working Party also identified four essential guarantees that must be satisfied when intelligence services access personal data, namely:

(a) Processing must be based on clear, precise and accessible rules.

(b) Necessity and proportionality in order to access to personal data.

(c) Independent oversight mechanism though either a judge or another independent body.

---

[24] For completeness, the validity of SCC and BCR as suitable mechanisms for transfers of personal data to the US is currently also being considered by the Article 29 Working Party.

[25] Statement of the Article 29 Working Party on the consequences of the Schrems judgment.

(d) Effective remedies available to individuals before an independent body.[26]

We consider in detail the features of the Privacy Shield Framework in section 6, where we also analyse its level of adequacy by reference to the CJEU's substantive criteria in its decisions in the *Digital Rights Ireland* and *Schrems* cases, and also take the four essential guarantees articulated in the Article Working Party statement into account.

[26] The Article 29 Working Party statement noted that the four essential guarantees should be respected whenever personal data is transferred from the EU to the US and to other third countries, as well as by EU Member States.

4. PROCESS FOR ADEQUACY FINDINGS UNDER THE DATA PROTECTION DIRECTIVE AND THE GDPR

The value of the Privacy Shield Framework as a mechanism to legitimise transfers of personal data from the EU to the US depends in large part on a future determination by the Commission that it provides an adequate level of protection for such data.

4.1 Process under the Data Protection Directive

As noted above, the Commission is empowered by Article 25(6) of the Data Protection Directive to determine whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. The effect of such a decision is that personal data can flow from each of the 28 EU Member States and three EEA member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguards being necessary.[27] The Commission has in the past recognised the need for a more extensive use of findings of adequate protection in respect of third countries so that more countries are considered adequate.[28]

The formal finding of adequacy is carried out following the procedure for 'community implementing measures' set out in Article 31 of the Data Protection Directive.[29] The Commission does not make such findings on its own but with input from:

(a) the Article 29 Working Party, which may deliver a non-binding opinion on the proposed decision (Article 30(1)(a) and (b) of the Data Protection Directive);

(b) the Committee of Member State representatives set up under Article 31 of the Data Protection Directive, which must approve the proposed decision and may refer the matter to the Council of Ministers for final determination (Article 31(2) of the Data Protection Directive); and

(c) the European Parliament and the Council, which are able to scrutinise whether the Commission has properly used its powers.[30]

The steps that are taken as part of the procedure for the Commission to adopt a decision based on Article 25(6) of the Data Protection Directive are as follows:

(a) Creation of a proposal from the Commission;

(b) Issuance of an Opinion of the Article 29 Working Party;

---

27 The Commission has so far recognized Andorra, Argentina, Canada (limited to commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection. The European Commission's adequacy decisions are available here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm. Note that these adequacy decisions do not cover data exchanges in the law enforcement sector. For special arrangements concerning exchanges of data in this field, see the PNR (Passenger Name Record) and TFTP (Terrorist Financing Tracking Programme) agreements.

28 See the First Report from the Commission on the implementation of the Data Protection Data Protection Directive of 15 May 2003 and more recently in the communication on a comprehensive approach on personal data protection in the European Union of 4 November 2010.

29 Under Article 31, the European Commission may take measures on specific topics identified in the Data Protection Directive, including in relation to adequacy findings. The scope of such measures can apply to an entire country (in the case of a decision that the laws of particular country provide an adequate level of protection, as noted above), organisations adhering a specific system (as was the case of the Safe Harbor Decision) or to organisations covered by a specific piece of legislation (as was the case in relation to the Commission's decision covering the adequacy of specific Canadian data protection legislation as applicable to private sector organisations, for example).

30 The procedure follows the rules set out in Regulation (EU) no 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers. For more information see the European Commission website at http://ec.europa.eu/transparency/regcomitology/index.cfm?do=implementing.home#6.

(c) Issuance of an Opinion of the Article 31 Committee delivered by a qualified majority of Member States, under the comitology 'examination procedure'; and

(d) Adoption of the Decision by the Commission.

At any time, the European Parliament and the Council may request the Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the Data Protection Directive.[31]

4.2 Process under the GDPR

As mentioned above, the regime created by the Data Protection Directive will be replaced by the GDPR in 2018. The official publication of the final text of the GDPR is expected to take place during the first half of 2016, but the substantive content of the GDPR agreed by the EU's legislative institutions is now set. Draft Article 41(1) of the GDPR (which will become Article 45(1) in the final text) states "*A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, or a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation*".

This effectively follows the principle under Article 25(6) of the Data Protection Directive referred to above. The GDPR (under draft Article 41, which will become Article 45 in the final text) goes on to establish a mechanism for the issuing, monitoring and amending of adequacy findings.

For completeness, under the GDPR, decisions adopted by the Commission on the basis of Article 25(6) of the Data Protection Directive will remain in force until amended, replaced or repealed by a new Commission decision.

[31] See the European Commission website, specifically the section on Commission decisions on the adequacy of the protection of personal data in third countries available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

5. CRITERIA LAID OUT BY THE CJEU

Even if the Commission adopts a decision that a cross-border data transfer mechanism provides an adequate level of protection, the CJEU can overrule such adequacy determinations by the Commission if they do not meet the standards set forth under EU law as interpreted by the CJEU in *Schrems*. It is therefore essential to assess the adequacy of the Privacy Shield by reference to the jurisprudence of the CJEU. We consider below the two key judgments from the CJEU examining respectively the Data Retention Directive and the Safe Harbor Decision in order to set out the criteria that the CJEU would likely use in the future to determine the validity of the Privacy Shield.

5.1 Relevant CJEU arguments in *Digital Rights Ireland*

Prior to *Schrems*, the CJEU considered certain EU data protection law aspects that are directly relevant to the issues at stake in the context of the assessment of the Privacy Shield. In *Digital Rights Ireland*[32], the CJEU examined whether or not the Data Retention Directive was valid in light of Articles 7, 8 and 11 of the Charter.[33] In determining the Data Retention Directive's invalidity, the CJEU laid out arguments which were later relied upon when examining the specific aspects that led to invalidity of the Safe Harbor Decision.

(a) Interference with fundamental rights

The CJEU established that the Data Retention Directive was an interference with Articles 7 and 8 of the Charter.[34] However, the CJEU acknowledged that even though the retention of data required by the Data Retention Directive constituted a particularly serious interference with those rights, it was not such as to adversely affect the essence of those rights, given that the Data Retention Directive did not permit the acquisition of knowledge of the content of the electronic communications as such.[35]

(b) No justification for the interference

Any law involving interference with fundamental rights must comply with Article 52 of the Charter. Article 52 of the Charter states that '*[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*'.

In considering the implications of the justification for interference under the Data Retention Directive, the CJEU accepted that the retention of data may be appropriate for attaining an objective of general interest pursued by the Data Retention Directive – to contribute to the fight against serious crime.[36] But any limitations to the Article 7 right to respect for private life must only be those that are strictly necessary.[37] In particular, the CJEU highlighted the following requirements for the purposes of lawfully justifying the interference with fundamental rights:

---

32 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others*, 8 April 2014, CJEU, C-293/12.

33 Article 11 is the right to freedom of expression and information which is not pertinent to the issues examined in this report.

34 *Digital Rights Ireland*, para 37.

35 *Digital Rights Ireland*, para 39.

36 *Digital Rights Ireland*, para 49.

37 *Digital Rights Ireland*, para 52.

(i) Clear and precise rules

The Data Retention Directive should have set down clear and precise rules governing the scope and application of the measure interfering with fundamental rights in question and the imposition of minimum safeguards so that persons whose data had been retained had sufficient guarantees to effectively protect their personal data against the risk of abuse and against unlawful access and use.[38] The CJEU emphasised that the need for such safeguards was all the greater where personal data was subjected to automatic processing and where there was a significant risk of unlawful access to such data.[39] But the Data Retention Directive did not set down any restricting rules on the interference (such as recognising limits around data protected by professional secrecy). Instead it required the retention of data on *all* persons using electronic communications even when there was no evidence to link a person with serious crime.[40]

(ii) Limits on access to data

Additionally, the Data Retention Directive did not set down any limits on access to the retained data by national authorities or limits on the subsequent use of the data.[41] There were no objective criteria in the Data Retention Directive to limit access to the data to what was strictly necessary.[42] In particular access to the retained data was not dependent on any prior review carried out by the courts or by an independent authority that checked that access to data was limited.

Since the Data Retention Directive did not lay down clear and precise rules governing the extent of the interference into the rights under the Charter and did not provide for sufficient safeguards to ensure the effective protection of data against the risk of abuse and against unlawful access and use, it was invalid.[43]

5.2 Court arguments and decision in *Schrems*

On 6 October 2015, the CJEU delivered its judgment in *Schrems*, the outcome of which was two-fold: (i) a DPA may examine whether the transfer of a person's data to a non-EU country complies with the requirements of the EU legislation on the protection of that data, and (ii) the Safe Harbor Decision was invalid.[44]

Crucially, in determining the invalidity of the Safe Harbor Decision, the CJEU laid out specific legal criteria that are to be used when assessing whether a particular data protection framework such as the Safe Harbor Framework is 'adequate' or, indeed, the adequacy of its successor in accordance with Article 25(6) of the Data Protection Directive.

(a) Independent oversight by EU Data Protection Authorities

The CJEU agreed with Advocate General Bot that Article 8(3) of the Charter guarantees the independence of DPAs whose power to investigate and provide oversight cannot be restricted.[45] Consequently, the Safe Harbor Decision did not prevent a DPA from

---

38 *Digital Rights Ireland*, para 54.
39 *Digital Rights Ireland*, para 55.
40 *Digital Rights Ireland*, para 58.
41 *Digital Rights Ireland*, para 61.
42 *Digital Rights Ireland*, para 62.
43 *Digital Rights Ireland*, para 65-66.
44 The CJEU is assisted by 11 Advocates General, who are responsible for presenting, with complete impartiality and independence, a non-binding 'Opinion' as to how the CJEU should decide the cases assigned to them. Advocate General Yves Bot, who was assigned to the *Schrems* case, issued his Opinion on 23 September 2015.
45 *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, CJEU, C-362/14, paras 47, 54-55.

examining a claim from an individual concerning the protection of his or her rights and freedoms.[46]

(b) Finding of adequacy and on-going verification

In considering whether a third country affords an adequate level of protection, the CJEU noted in *Schrems* that Article 25(2) of the Data Protection Directive indicates that adequacy shall be assessed in the light of all the circumstances.[47] Specifically, where the Commission assesses a third country to consider whether the third country is adequate, the third country must ensure an adequate level of protection by reason of its domestic law or international commitments for the protection of the private lives and basic freedoms and rights of individuals.[48] The intention is to ensure that the high level of protection afforded to personal data in the EU continues where personal data is transferred to a third country.[49] Whilst allowing that the third country is not required to ensure a level of protection identical to that found in the EU, the CJEU indicated that adequacy must be understood to require the third country to ensure an 'essentially equivalent' level of protection as that found in the EU under the Data Protection Directive read in the light of the Charter.[50]

Therefore the Commission in considering whether the Safe Harbor Framework was adequate was required to assess the content of the rules in the US and the practices designed to ensure compliance with those rules.[51] Furthermore, the CJEU indicated that the Commission was also required to periodically check whether the adequacy finding was still factually and legally justified.[52] Any discretion available to the Commission to consider the adequacy of the third country should be limited as the review of the requirements should be strict.[53]

(c) Deficiencies of the Safe Harbor Decision

In the CJEU's view, the Safe Harbor Decision suffered from certain deficiencies. The fact that Safe Harbor was a self-certification scheme was not in itself contrary to the basis laid down in Article 25(6) of the Data Protection Directive for an adequacy finding, but it made it even more important that there were effective detection and supervision mechanisms in place.[54] A related observation was that the Safe Harbor Decision was only applicable to commercial organisations and so had no effect over US authorities who accessed personal data held by Safe Harbor registered organisations.[55]

Moreover, the Safe Harbor Decision did not set out in sufficient detail why the Commission considered that the US ensured an adequate level of protection for personal data.[56] Additionally, where there was a conflict between the requirements of the Safe Harbor Privacy Principles and US law, the Safe Harbor Decision clearly stated that US law would take primacy.[57]

---

46 *Schrems*, para 56 and 99.
47 *Schrems*, para 70.
48 *Schrems*, para 71.
49 *Schrems*, para 72.
50 *Schrems*, para 73.
51 *Schrems*, para 75.
52 *Schrems*, para 76.
53 *Schrems*, para 78.
54 *Schrems*, para 81.
55 *Schrems*, para 82.
56 *Schrems*, para 83.
57 *Schrems*, para 85.

(d) Interference with fundamental rights

As discussed above, any law involving interference with fundamental rights must comply with Article 52 of the Charter. The Commission recognised the need for there to be certain derogations from the Safe Harbor Privacy Principles since the wording in the fourth paragraph of Annex I of the Safe Harbor Decision indicates that adherence to the Safe Harbor Privacy Principles may be limited in certain circumstances e.g. to the extent necessary to meet national security, public interest, or law enforcement requirements (the "**Derogation Provision**").

In the CJEU's view the general nature of the Derogation Provision enabled interference with the fundamental rights under the Charter.[58] To add to the concern, the CJEU found a lack of accountability mechanisms set out in the Safe Harbor Decision since the Safe Harbor Decision did not refer to any US rules to limit interference or to the existence of any effective legal protection against such interference.[59] Moreover, procedures before the FTC and private dispute resolution mechanisms could not be used to examine the interference with fundamental rights.

(e) No justification for the interference

Any law involving interference with fundamental rights must satisfy Article 52 of the Charter and '*lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data*'.[60] Such safeguards are even more important where there is a significant risk of unlawful access.

Any derogation from the protection of the fundamental right to privacy must be only in so far as is strictly necessary.[61] With reference to *Digital Rights Ireland*, the CJEU underlined that legislation (whether EU or non-EU) is not limited to what is strictly necessary where it authorises '*on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail*'.[62]

Legislation permitting public authorities to have generalised access to the content of electronic communications compromises the essence of the fundamental right under Article 7 in the eyes of the CJEU.[63]

(f) No right to a remedy

Additionally the CJEU found that the Safe Harbor Decision did not give individuals the right to pursue a legal remedy in order to access their data, obtain rectification of their data or obtain erasure of their data. Therefore the Safe Harbor Decision did not comply with Article 47 of the Charter.[64]

---

58 *Schrems*, para 87.
59 *Schrems*, para 88-89.
60 *Schrems*, para 91 and *Digital Rights Ireland.*
61 *Schrems*, para 92.
62 *Schrems,* para 93.
63 *Schrems*, para 94.
64 *Schrems*, para 95.

5.3 **Summary of criteria from CJEU**

The CJEU judgments referred to above are particularly relevant to the assessment of the adequacy of the Privacy Shield because they set out a number of principles and criteria against which the Privacy Shield will be legally scrutinised. Taking all such jurisprudence into account, we consider that for the purposes of a valid adequacy determination by the Commission, the Privacy Shield must be able to meet the following specific criteria:

- Unrestricted and independent oversight by the DPAs to examine a claim from an individual concerning the protection of his or her right to respect for private and family life and the right to the protection of personal data (Articles 7 and 8 of the Charter). This should be extensively interpreted, in the sense that such competence by the DPAs must have a practical application and be able to lead to the resolution of the matter.

- The Commission must also be entitled to periodically check whether the adequacy finding is still factually and legally justified.

- Any interference with Articles 7 and 8 of the Charter taking place in connection with the transfer of personal data to the US pursuant to the Privacy Shield must comply with Article 52 of the Charter so that:

    - It must be provided for by law, which should be validly enacted and enforceable.

    - It must respect the essence of the rights and freedoms recognised by the Charter, which is underpinned by the principles of democracy and the rule of law.

    - It must be proportionate so that the law must be appropriate to attain its legitimate objectives.

    - It must be limited to what is strictly necessary.

    - It must genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

    - The scope of the interference must be expressed in clear and precise rules.

    - There are minimum safeguards to ensure sufficient guarantees to protect the personal data against abuse and unlawful access and use.

    - There is proper accountability for third country public authorities accessing the data.

    - There are objective criteria determining the limits of access by public authorities to the data and its subsequent use for specific and strictly restricted purposes.

- Individuals must have a right to pursue effective legal remedies before an independent and impartial tribunal previously established by law, as enshrined in Article 47 of the Charter.

6. ADEQUACY ANALYSIS OF THE PRIVACY SHIELD

6.1 Privacy Shield Principles

The Privacy Shield Framework is structured around 7 Principles and 16 Supplemental Principles ("**Privacy Shield Principles**"). While the Privacy Shield Principles follow the structure of the Safe Harbor Framework, some of the provisions have been expanded. The Principle that has been altered most significantly is 'Recourse, Enforcement and Liability' which was 'Enforcement' under the Safe Harbor Framework. An analysis of the Principles is set out at (a) – (g) below.

(a) Notice

Summary: The Notice principle under the Privacy Shield Framework requires organisations to provide more specific information in their privacy policies.

The Notice principle under the Safe Harbor Framework merely stated that a member was required to "*inform individuals about the purposes for which it collects and uses information about them, how to contact the information with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.*" For the most part, organisations complied with this requirement by describing these categories of information at a high level in their published Safe Harbor privacy policies.

The Notice principle under the Privacy Shield Framework is much more specific. In particular, this principle lists thirteen different details that participants must include in their published privacy policies, including (i) any relevant establishment in the EU that can respond to inquiries or complaints, (ii) the independent dispute resolution body designated to address complaints, a hyperlink to the complaint submission form of that dispute resolution body, and the possibility, under certain circumstances, for EU individuals to invoke additional binding arbitration; and (iii) the possibility that the organisation may be held liable for unlawful transfers of personal data to third parties.

(b) Choice

Summary: The Choice principle under the Privacy Shield Framework remains largely unchanged from the Safe Harbor Framework.

The Choice principle requires participants to provide a mechanism for individuals to opt out of having personal information disclosed to a third party or used for a materially different purpose than that for which it was provided, although the Privacy Shield Framework clarifies that this option need not be provided when the disclosure is made to a third-party service provider that will use the information solely under the instructions of the organisation (i.e. data processors, in European terms). As with the Safe Harbor Framework, the Privacy Shield Framework also requires covered organisations to obtain affirmative express consent from individuals prior to sharing sensitive information with a third party or using it for a purpose other than for which it was initially collected.

(c) Accountability for Onward Transfer

Summary: This principle represents important new requirements for Privacy Shield organisations when transferring data to third parties.

While similar to the 'Onward Transfer' Principle under the Safe Harbor Framework, this principle is expanded to add requirements on transfers to third parties. For instance, there is now a requirement for the Privacy Shield organisation to enter into a contract with third party controllers to which it transfers personal data. Additionally, there are further obligations on Privacy Shield organisations that transfer personal data to agents or service providers. For instance, the organisation must ascertain that the agent is required to provide at least the same level of privacy protection as required by the Privacy Shield Principles.

(d) Security

Summary: Data security requirements are unchanged under the Privacy Shield Framework.

Organisations joining the Privacy Shield Framework must take reasonable and appropriate measures to protect EU personal data from loss, misuse and unauthorised access, disclosure, alteration, and destruction, taking into "due account" the risks involved in the processing and the nature of the personal data.

(e) Data Integrity and Purpose Limitation

Summary: This principle now requires a Privacy Shield organisation to adhere to the Privacy Shield Principles for as long as it retains the relevant data, regardless of whether the company withdraws from the framework.

This principle retains all of the obligations under the analogous provision of the Safe Harbor Framework, requiring the organisation to take reasonable steps to limit processing to the purposes for which it was collected, and to ensure that personal data is reliable for its intended use, accurate, complete, and current. It explicitly adds that an organisation must adhere to the Privacy Shield Principles for as long as it retains such information, regardless of whether the company withdraws from the framework.

(f) Access

Summary: The Access principle is effectively the same as it was under the Safe Harbor Framework.

Organisations must provide a mechanism by which individuals may request personal information related to them be corrected, amended, or deleted, and obtain confirmation of whether an organisation is processing information related to them.

(g) Recourse, Enforcement and Liability

Summary: This principle has been significantly expanded to include new recourse mechanisms individuals can pursue to resolve claims against Privacy Shield organisations, including a new arbitration mechanism and an expanded role for the DoC to facilitate dispute resolution between individuals and Privacy Shield organisations.

Under this principle '*effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the*

organisation when the Principles are not followed'.[65] At a minimum such mechanism must include Individual Redress, Consequences for Non-Compliance and Compliance Verification.

(i) Individual Redress

Where an individual consumer complains to the Privacy Shield organisation, the organisation must respond to the individual within 45 days of receiving the complaint.[66] As was the case under the Safe Harbor Framework, Privacy Shield organisations must subscribe to an independent recourse mechanism to resolve any complaints from EU individuals that the organisation is unable to resolve itself. The recourse mechanism must be impartial, readily available and free for the individual. Usually this will involve registering with a third party independent dispute resolution body. There is an explicit reference to the possibility that damages could be awarded to individuals where applicable law or private sector initiatives provide.[67] Both Privacy Shield organisations and the independent dispute resolution body must respond promptly to requests from the DoC.

Additionally, an individual may complain to their local EU DPA about a Privacy Shield organisation's processing of their personal data and the DPA may then raise the matter with the DoC. The DoC and FTC are obligated to investigate and resolve complaints forwarded by a DPA.

Where there are claims that are still not satisfactorily resolved, an individual may resort to an arbitration option with arbitrators appointed to sit on a Privacy Shield Panel. The DoC and Commission will designate a pool of 20 arbitrators and the parties to a dispute may then select either one or three arbitrators. The arbitrators can determine whether an organisation has violated its obligations under the Privacy Shield Principles but cannot consider questions relating to the Derogation Provision or any concern about the adequacy of the Privacy Shield Framework. Any ruling from the Privacy Shield Panel can impose individual-specific, non-monetary equitable relief to remedy non-compliance with the Privacy Shield Framework.

(ii) Consequences for non-compliance

While the powers of the FTC and DoT under the Safe Harbor Framework also subsist under the Privacy Shield Framework, there are additional consequences for Privacy Shield organisations. The organisation remains liable for its service providers' failure to comply with the Principles unless the organisation can show it was not responsible for the event giving rise to the damage. There is also potentially greater transparency since an organisation that is subject to a FTC or court order based on non-compliance is required to make public any relevant Privacy Shield-related sections of a compliance or assessment report submitted to the FTC.

---

65 Annex II, EU-US Privacy Shield Framework Principles issued by the US Department of Commerce, Section II, para 7 (a).

66 Annex II, Section III, para 11 (d).

67 Annex II, Section II, para 7 (a) (i).

(iii) Compliance verification

Organisations can use self-assessments or outside assessments in order to follow up their procedures to verify compliance including any instance of previous non-compliance.[68] Organisations must also retain their records demonstrating their implementation of the Privacy Shield Principles as these could be required in the course of an investigation and could ultimately be made public.

The newly cast Recourse, Enforcement and Liability Privacy Principle under the Privacy Shield reflects the commitment of the Commission and DoC to ensure that EU individuals have sufficient redress mechanisms under the Privacy Shield Framework.

(h) Derogations

Significantly, the Privacy Shield Framework follows the same position relating to limitations or derogations from the Principles as seen in the Safe Harbor Decision. So the section in Annex II giving the Overview to the Privacy Shield Principles includes at section I.5 verbatim what was previously in the fourth paragraph of Annex I of the Safe Harbor Framework setting out the derogations from compliance, referred to as the Derogation Provision in section 5 of this report.

6.2 **Administration and supervision**

The Privacy Shield will be administered primarily by the DoC. The FTC and DoT will continue to play a role in enforcing the Privacy Shield Framework against the organisations that the FTC and DoT respectively have power to regulate. Letters in Annex IV and Annex V in the Privacy Shield Framework provide reassurances from the FTC and DoT that they will enforce compliance with the Privacy Shield Principles.

Administration and supervision of the Privacy Shield Framework will be carried out in the following key ways:

(a) Privacy Shield website

The DoC will continue to maintain a list of currently certified Privacy Shield organisations but will update the existing Safe Harbor website to include:

- A record of organisations that had been Privacy Shield certified but have been removed and identifying the reason for the removal.
- A prominent reminder that organisations removed from the Privacy Shield list must continue to apply the Privacy Shield Principles to the Privacy Shield data they continue to maintain in the US.
- A link to the list of Privacy Shield-related cases on the FTC website.
- Different sections of the website tailored to EU individuals, EU businesses and US businesses.

(b) Expanding efforts to follow up with organisations that have been removed

The DoC will be more proactive in notifying organisations that if they are removed from the Privacy Shield list for 'persistent failure to comply', the organisation is not

[68] Annex II, Section II, para 7.

entitled to retain Privacy Shield data. DoC will also send questionnaires to organisations whose self-certification have lapsed or have voluntarily withdrawn from the Privacy Shield to verify how the organisation will continue to protect Privacy Shield data.

(c) Searching for and addressing false claims of participation

The DoC will be more proactive in searching for and addressing false claims that organisations maintain Privacy Shield status which will include spot-checks of the privacy notices of previously certified organisations, conducting internet searches to identify where images of the Privacy Shield certification mark are being displayed to check whether such use is valid, as well as reviewing and addressing complaints about false claims of participation promptly.

(d) Conducting periodic *ex officio* compliance reviews and assessments

The DoC will, in consultation with DPAs if appropriate, conduct reviews of an organisation's Privacy Shield compliance when (i) the DoC receives a specific non-frivolous complaint about the organisation's compliance, (ii) the organisation does not respond satisfactorily to DoC inquiries, or (iii) there is credible evidence that the organisation does not comply with the Privacy Shield Principles. The FTC will also give priority consideration to referrals of non-compliance with the Privacy Shield Principles to determine whether the organisation has violated Section 5 of the Federal Trade Commission Act (i.e. by undertaking unfair and deceptive practices) or other law.

(e) Increasing cooperation with European Data Protection Authorities

There will be an increase in direct working arrangements between the DoC and DPAs including conducting compliance reviews and facilitating the resolution of complaints based on referrals from the DPAs.

(f) Annually reviewing the functioning of the Privacy Shield

Every year representatives of the Privacy Shield stakeholders – including the DoC, FTC, Commission and DPAs – will meet to discuss the continuing efficacy of the framework. In addition, the Commission will continuously monitor the functioning of the Privacy Shield Framework with a view to assessing whether the US continues to ensure an adequate level of protection. The Commission is also entitled to suspend, amend or repeal its adequacy decision in cases of systematic failures or where the US public authorities do not comply with their representations and commitments.

6.3 **Limitations on US Government access to data**

Whereas the Safe Harbor Decision did not refer to any specific limitations on US government access to data transferred to the US under the Safe Harbor Framework, the Privacy Shield Framework provides considerable detail concerning the restrictions and limitations in place under US law. Other than the familiar statement in the Derogation Provision that adherence to the Privacy Shield may be limited to the extent necessary to meet national security, public interest, or law enforcement requirements, the limitations on US government access are not expressed within the Privacy Shield Principles as such, since the US government and its agencies are not subject to the Privacy Shield Framework. But it is evident that a considerable amount of effort has been deployed to acknowledge and explicate limitations on the access rights of US government to personal

data transferred under the Privacy Shield Framework. Indeed, these limitations are an essential component of the Privacy Shield Framework.

The Privacy Shield Framework documentation jointly published by the Commission and the DoC includes letters from:

- The Office of the Director of National Intelligence ("**ODNI**") – which serves as the head of the US intelligence community and acts as the principal advisor to the President and the National Security Council on intelligence issues – regarding the safeguards and limitations applicable to US national security authorities ("**ODNI Letter**")[69];
- US Secretary of State, Kerry, describing the commitment of the Department of State to establish a new Privacy Shield Ombudsperson for submission of inquiries regarding the US' signals intelligence practices ("**Ombudsperson Letter**")[70]; and
- The US Department of Justice regarding the safeguards and limitations on US government access for law enforcement and public interest purposes ("**Justice Letter**").[71]

Taken together these letters are presented as binding commitments from the US government that there are meaningful and effective limitations on the US government's access to data transferred under the Privacy Shield. These limitations are set out in detail below.

(a) Access and use by US public authorities for national security purposes

(i) Limitations

US intelligence agencies access data for national security purposes under a complex legal framework which includes procedures, rules and guidelines establishing restrictions on how data can be accessed and used. They may only seek access to personal data transferred under the Privacy Shield if their request complies with the Foreign Intelligence Surveillance Act ("**FISA**") or is made by the Federal Bureau of Intelligence based on a National Security Letter ("**NSL**").[72] Recent legal changes have established further restrictions on the access and use of data. In particular, the USA FREEDOM Act, enacted in June 2015, prohibits the collection in bulk of records where such collection is based on Section 402 of FISA (which provides procedures for the government's collection of certain communications metadata), Section 501 of FISA (which provides procedures for the government's collection of "tangible things," including phone metadata) or through the use of NSLs.[73]

- PPD-28: Privacy Principles

US President Obama issued Presidential Policy Directive 28 ("**PPD-28**") in January 2014, which set out further principles and restrictions on the use of signals intelligence data for all people, regardless of nationality or origin. PPD-28 stipulates that, inter alia:

---

69 Annex VI.
70 Annex III.
71 Annex VII.
72 ODNI Letter, p. 2.
73 Draft Commission Implementing Decision, recital 66.

- All persons should be treated with dignity and respect regardless of their nationality or wherever they might reside;
- All persons have legitimate privacy interests in the handling of their personal information;
- Collection of signals intelligence must be based on statute or Presidential authorisation and be carried out in accordance with the US Constitution and US law;
- Privacy and civil liberties are integral considerations in planning US signals intelligence activities and signals intelligence shall only be collected where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions;
- Signals intelligence activities shall be as tailored as feasible so that in determining whether to collect signals intelligence, the US shall consider the availability of other sources; and
- Signals intelligence activities must include appropriate safeguards for the personal information of all individuals including periodic auditing against the standards required by PPD-28.

The ODNI Letter contains assurances that PPD-28 and its associated processes and procedures enabling the collection, retention and dissemination of foreign intelligence provide important privacy protections for all individuals, regardless of nationality.[74]

PPD-28 indicates that signals intelligence activities should be as tailored as feasible and the ODNI Letter emphasises that this requirement applies to the manner in which signals intelligence is collected, as well as to what is actually collected.[75] Additionally, wherever practical, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (e.g. specific facilities, selection terms and identifiers). PPD-28 sets out further retention and dissemination limitations on data collected through signals intelligence activities which apply to persons of any nationality. For instance, it states that US agencies must usually delete non-US personal information collected through signals intelligence five years after collection unless the Director of National Intelligence expressly determines that the information remains relevant for authorised foreign intelligence requirements or continued retention is in the interests of national security.

- PPD-28: Bulk data collection

PPD-28 does not forbid the bulk collection of signals intelligence data since the US government considers it to be necessary in order to locate new or emerging threats which are often hidden within the large and complex system of modern global communications[76]. But the ODNI Letter emphasises that PPD-28 directs US agencies to prioritise targeted signals intelligence rather than bulk signals intelligence.

---

74 ODNI Letter, p.9.

75 ODNI Letter, p. 3.

76 Presidential Policy Directive/PPD-28, January 17, 2014, section 2, p. 3; ODNI Letter p.3.

Although US national security agencies may continue to collect bulk signals intelligence data, PPD-28 limits the use that US agencies can make of the data collected. Specifically, where non-publicly available signals intelligence is collected in bulk, PPD-28 directs US authorities to only use that data for the purposes of detecting and countering six narrow categories of threats:

- Espionage and other threats and activities directed by foreign powers or their intelligence services against the US and its interests;
- Threats to the US and its interests from terrorism;
- Threats to the US and its interests from the development, possession, proliferation, or use of weapons of mass destruction;
- Cybersecurity threats;
- Threats to US or allied Armed Forces or other US or allied personnel; and
- Transnational criminal threats.

PPD-28 mandates that signals intelligence collected in bulk cannot be used to silence free speech or unfairly discriminate against individuals based on race, ethnicity, gender, sexual orientation or religion. PPD-28 is clear that the limits set out are intended to protect the privacy and civil liberties of all persons. It is however noteworthy that the limitations on bulk collection do not apply to signals intelligence data temporarily acquired to facilitate targeted collection.[77]

- FISA: Section 702

Section 702 of FISA also has come under scrutiny after the Snowden revelations. In general, FISA governs the surveillance of and the collection of evidence about persons suspected of being part of a terrorist organisation or acting as spies for foreign governments.[78] Such requests are subject to prior authorisation by the FISC, a court comprised of a rotating panel of existing, independent, lifetime-appointed federal judges to evaluate whether requests for surveillance meet legal requirements. Decisions of the FISC are appealable to the Foreign Intelligence Surveillance Court of Review, also a panel of existing federal judges, whose decisions in turn are appealable to the US Supreme Court.

Section 702 does not give the US government carte blanche to seize whatever data it wants. Collection of data under Section 702 of FISA is focused on the collection of "foreign intelligence information" from individually identified legitimate targets. Furthermore such collection is authorised under statute, is subject to independent judicial supervision, is subject to review and oversight from within the executive branch as well as Congress and is subject to PPD-28 requirements.[79]

---

77 PPD-28, Footnote 5.

78 Winston Maxwell & Christopher Wolf, *A Sober Look at National Security Access to Data in the Cloud*, 23 July 2014.

79 See *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013).

Section 702 only permits the targeting of "foreign intelligence information". By definition, foreign intelligence information is limited to information related to (1) acts of terrorists and other third parties seeking to harm the security of the US, and (2) national defence, security, or foreign affairs. Authority to gather these types of information is reserved and exercised by all major sovereign powers, not just the US.[80] Moreover, these categories of information must be ascribed to a "foreign power or foreign territory." This means that private citizens' business records, academic research, and political opinions, among other records, do not constitute "foreign intelligence information."

To make use of Section 702, the Attorney General and the Director of National Intelligence ("**DNI**") must jointly and under oath submit a certification to the FISC attesting, inter alia, that a significant purpose of the surveillance is to obtain foreign intelligence information. Absent emergency circumstances, this certification must be submitted to and approved by the FISC prior to conducting the surveillance. Once the FISC approves this certification, the government is permitted to direct a service provider to conduct the authorised surveillance for a one-year period.

Companies that are subject to such directives can immediately challenge the lawfulness of the directive before the FISC, and can appeal such decisions to the Court of Review and petition the Supreme Court. In addition, the government is required to declare in advance whenever it wishes to use any information collected through Section 702 in a judicial or administrative proceeding, and if so, any affected person or entity can challenge the lawfulness of the acquisition before the government introduces it as evidence.

Information collected under Section 702 of FISA can only be reviewed by intelligence personnel who have been trained in privacy-protective minimisation procedures and will only use the data to identify foreign intelligence information or evidence of a crime.[81]

By statute, the United States has established an independent Privacy and Civil Liberties Oversight Board ("**PCLOB**") whose mandate is to (1) review and analyse actions the executive branch takes to protect the nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties, and (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the nation from terrorism.[82] In this role, the PCLOB in 2014 reviewed and issued a report regarding the operation of Section 702,[83] which included an analysis of the treatment of non-US persons under the law. In its report, the PCLOB concluded that the limitations in place under Section 702 'do not permit unrestricted collection of information about foreigners'.[84] Collections under Section 702 must be authorised by statute, fall within the certifications approved by FISC and focus on targeting

---

80 Maxwell & Wolf, p. 3.

81 ODNI Letter, p. 11.

82 42 U.S.C. § 2000ee.

83 PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2 July 2014, *available at* https://www.pclob.gov/library/702-Report.pdf.

84 ODNI Letter, p. 10.

particular persons about which a determination has been made.[85] The PCLOB also concluded that Section 702 contains other legal protections for the privacy of non-US persons, including penalties for government employees who engage in improper information collection practices statutory limitations on the use of information acquired from FISA-related surveillance except for lawful purposes, and special protections in connection with legal proceedings under which an aggrieved person is required to be notified prior to the disclosure or use of any Section 702-related information in any federal or state court – both applicable regardless of whether the victim is a US person or non-US person.

(ii) Effective legal protection

At a high level, the National Intelligence Priorities Framework ("**NIPF**") lays down the intelligence priorities of the US and the National Signals Intelligence Committee ("**SIGCOM**") is responsible for translating these priorities into signals intelligence collection and overseeing its collection across the Intelligence Community.[86] All US agencies that wish to collect signals intelligence must submit requests to SIGCOM who must ensure that such requests are consistent with the NIPF and, inter alia, will not present an unwarranted risk to privacy and civil liberties.

Significantly, decisions made by US agencies about what is feasible or practical as required under PPD-28 are not at the discretion of individuals but are set out in the (publicly available) policies that US agencies are required to implement under PPD-28.[87] Additionally, all US intelligence priorities are established by senior personnel.[88] The ODNI Letter indicates that the procedures it lists demonstrate a clear commitment to prevent arbitrary and indiscriminate collection of signals intelligence information and to implement the principle of reasonableness.[89]

In addition, the ODNI Letter provides further details of formal compliance and oversight mechanisms for US agencies involved in foreign intelligence and signals intelligence data collection. These are listed as:

- The President's National Security Advisor, in consultation with the DNI, will annually review the permissible uses of signals intelligence collected in bulk to see whether they should be changed.
- Oversight personnel within the Intelligence Community.
- Oversight from the Department of Justice and Department of Defense.
- Each element of the Intelligence Community[90] has an Office of the Inspector General (an independent function) with responsibility for oversight of foreign intelligence activities.

---

85 ODNI Letter, p. 10-11.
86 ODNI Letter, p. 5.
87 ODNI Letter, p. 3.
88 ODNI Letter, p. 6.
89 ODNI Letter, p.6.
90 To be understood as the term is used in Executive Order 12333.

- ODNI's Civil Liberties and Privacy Office is required to ensure that the Intelligence Community operates in a manner that advances national security while protecting civil liberties and privacy rights.
- The PCLOB, an independent body, analyses and reviews counterterrorism programmes and policies to ensure they adequately protect privacy and civil liberties.
- The FISC, which is responsible for oversight and compliance of any signals intelligence collection conducted under the FISA.
- US Congress and the House and Senate Intelligence and Judiciary Committees, which have the authority to pass legislation governing access to data by US government agencies, such as Section 702.

Less formal oversight and compliance mechanisms that the ODNI Letter refers to include regular checks by the National Security Agency on their collection process to ensure their findings match the priorities, monitoring by the DNI of particularly sensitive signals intelligence, and an annual review by the ODNI of the Intelligence Community's resources against the NIPF. PPD-28 also requires US agencies to carry out periodic audits and reviews of their practices for protecting personal information contained in signals intelligence.

Oversight of the use of Section 702 FISA is extensive as agencies complying with FISA have multiple layers of internal review (including by Inspectors General) and the Department of Justice and ODNI closely scrutinize the use of Section 702. Agencies must report potential incidents of noncompliance to the FISC, the President's Intelligence Oversight Board and Congress who have the power to investigate and seek remedies.

The FISC plays a central role in ensuring that the certifications, targeting and minimisation procedures comply with statutory requirements. Under the USA FREEDOM Act the FISC is now explicitly authorised to appoint an external lawyer as an independent advocate on behalf of privacy concerns in cases that present novel or significant legal issues.[91] Congress is also involved in exercising oversight through statutorily required reports to the Intelligence and Judiciary Committees as well as briefing and hearings.

(iii) Ombudsperson

The US government has created an entirely new role of Privacy Shield Ombudsperson ("**Ombudsperson**"). The purpose of the Ombudsperson, set out in the Ombudsperson Letter in Annex III, is to be a contact point for EU authorities to submit requests on behalf of EU individuals relating to US signals intelligence practices. The Ombudsperson is independent from the Intelligence Community and reports directly to the US Secretary of State. The Ombudsperson is responsible for ensuring that EU individuals who submit complaints to their DPA about US signals intelligence receive an appropriate response in accordance with applicable laws and policies. In particular the response must confirm whether the complaint has been

[91] Section 401 of the USA FREEDOM Act, P.L. 114-23

properly investigated and whether US law and related directives, orders and policies providing limitations and safeguards have been complied with.

Crucially, in the event of non-compliance with such laws and related directives, orders and policies providing limitations and safeguards, the Ombudsperson's response must confirm that such non-compliance has been remedied. The response will not confirm or deny whether the individual was the target of surveillance nor will it confirm any remedy that was applied. The Ombudsperson's role is strictly in relation to signals intelligence and she will not consider claims about the Privacy Shield's legal standing under EU data protection law.

For completeness, the Ombudsperson mechanism will also operate in respect of transfers carried out on the basis of SCC and BCR.

(iv) Transparency

Changes brought in through the USA FREEDOM Act increased transparency over surveillance and national security activities by US agencies. For example, the DNI, in consultation with the Attorney General, is required to either declassify or publish an unclassified summary of each decision, order or opinion issued by the FISC or Foreign Intelligence Surveillance Court of Review that includes a significant construction or interpretation of any provision of law.[92] The US government must also annually disclose to Congress and to the public the number of FISA orders and certifications sought and received as well as the estimated number of US and non-US persons targeted. Companies may also publish their own transparency reports setting out the number of FISA orders, directives or NSLs they receive from the US government and the limited number of customers whose records have been sought.[93]

In addition, there is a new FAQ in the Privacy Shield Principles which allows and encourages Privacy Shield organisations to voluntarily provide transparency by issuing periodic transparency reports on the number of requests for personal data that they receive from public authorities, in compliance with applicable law.[94]

(v) Individual redress

An individual can seek relief in US courts if he or she can establish standing to bring a claim to challenge unlawful electronic surveillance under FISA. FISA allows individuals subjected to unlawful electronic surveillance to sue US government officials for damages. As described above, where the US government wishes to use or disclose information obtained or derived from electronic surveillance under FISA against an individual in judicial or administrative proceedings in the US, it must provide advanced notice of its intent to the tribunal and the individual who then has the right to challenge the legality of the surveillance.[95] There are additionally criminal penalties under FISA for individuals who intentionally

---

92 ODNI Letter, p. 14.
93 ODNI Letter, p. 14.
94 Annex II, Section III, para 16 – Access Requests by Public Authorities.
95 ODNI Letter, p. 16.

engage in unlawful electronic surveillance under colour of law or who intentionally use or disclose information obtained by unlawful surveillance.

EU-based individuals and citizens may also seek legal redress under US laws including the Computer Fraud and Abuse Act, Electronic Communications Privacy Act and Right to Financial Privacy Act where applicable.

(b) Access and use by US public authorities for law enforcement and public interest purposes

In the Justice Letter, the US Department of Justice provides an overview of the primary investigative tools used to obtain data from companies in the US for criminal law enforcement or public interest purposes. These powers include obtaining data held by Privacy Shield organisations, and are similar to many of the investigative tools available to European law enforcement authorities and prosecutors.[96]

(i) Limitations and oversight on law enforcement

Federal prosecutors and federal investigative agents have the power to compel production of documents and records from US companies for criminal investigative purposes through compulsory legal processes such as grand jury subpoenas and search warrants.[97] Criminal subpoenas are used to support targeted law enforcement investigations and grand jury subpoenas are official requests from a grand jury to support its investigation into a particular suspected violation of criminal law. A subpoena cannot be overbroad in scope or be oppressive or burdensome but could require that a company disclose certain business records or other electronically stored information, but only if relevant to a legitimate investigation. Similarly an administrative subpoena requires recipients to disclose information for the purpose of investigations carried out by US authorities into, for instance, health care fraud or child abuse. A recipient can file a motion to challenge a subpoena.

Law enforcement may also access data through court orders for pen register and trap and traces, under the Electronic Communications Privacy Act (usually under a warrant from a judge), court orders for surveillance under Federal Wiretap law, or search warrants where a judge has authorised the warrant.

The Attorney General has also issued guidelines that place further limits on law enforcement access to data and contain privacy and civil liberty protections. For instance, requiring the FBI to use the least intrusive investigative methods feasible taking into account the effect on privacy and civil liberties and the potential damage to reputation.

(ii) Limitations and oversight on access for public interest purposes

Civil and regulatory authorities may issue subpoenas to require US companies to disclose business records or electronically stored information but are limited in obtaining subpoenas by their powers under statute and by independent judicial review of subpoenas prior to potential

[96] *See* Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, 18 July 2012.
[97] Justice Letter, p. 2.

judicial enforcement. Furthermore, agencies can only seek access to data that is relevant to matters within their scope of authority to regulate. A recipient can file a motion to challenge these subpoenas as well.

US companies may also challenge data requests from administrative agencies if there is a specific sector statute giving the company grounds for challenge such as under the Bank Secrecy Act or Fair Credit Reporting Act.

6.4 **European Commission's draft adequacy finding**

As explained above, under Article 25(6) of the Data Protection Directive, the Commission may find that a third country ensures an adequate level of protection within the meaning of Article 25(2) by reason of its domestic law or of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals. Under Article 25(2) the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations. The draft adequacy finding in the Privacy Shield Framework published by the Commission reveals the Commission's assessment of the various elements of the documentation.

(a) Privacy Shield

(i) *Privacy Principles* (recitals 16-23)

The Commission comments on each of the revised Privacy Shield Principles.

In the Commission's view, the Privacy Shield Principles issued by the DoC "*as a whole ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the substantive basic principles laid down in Directive 95/46/EC*."[98]

(ii) *Transparency and Administration of the EU-U.S. Privacy Shield* (recitals 24-28)

The Commission notes the greater scrutiny that will be applied by the DoC to organisations seeking to participate in the Privacy Shield and the more active role for the DoC in monitoring and enforcing non-compliance.

The Commission considers that "*the effective application of the Privacy Principles is guaranteed by the transparency obligations and the administration of the Privacy Shield by the Department of Commerce*".[99]

(iii) *Compliance review and complaint handling* (recitals 29-51)

The Commission notes the avenues open for EU individuals to pursue remedies against Privacy Shield organisations. The complaint handling process that organisations have to comply with requires them to demonstrate accountability to the DoC and independent dispute resolution bodies. There are also references to the obligation on the DoC to ensure organisations continue to protect personal data transferred under the Privacy Shield even after the organisation is no longer part of the Privacy

[98] Draft Commission Implementing Decision, recital 49.
[99] Draft Commission Implementing Decision, recital 50.

Shield framework, and on the FTC to prioritise referrals of an organisation's non-compliance. Organisations may also voluntarily submit to the oversight by DPAs. Where none of the other redress mechanisms have satisfactorily resolved the complaint, the Commission notes the 'last resort' arbitration option that is open to individuals to pursue.

The Commission also reconfirms the ability of a DPA to suspend a data transfer if the DPA, on examining a claim from an EU individual, considers that the personal data transferred to a US organisation is not afforded an adequate level of protection.

In the Commission's view "*taken as a whole, the oversight and recourse mechanisms provided for by the Privacy Shield enable infringements of the Privacy Principles by Privacy Shield organisations to be identified and punished in practice and offer legal remedies to the data subject to gain access to personal data relating to him and, eventually, to obtain the rectification or erasure of such data*".[100]

(b) Access and use of personal data transferred under the EU-US Privacy Shield by US public authorities

The Commission refers to the letters - the ODNI Letter, Justice Letter and Ombudsperson Letter – as forming part of the Privacy Shield Decision to enhance transparency "*and to reflect the legal nature of these commitments*" indicating clearly that the Commission expects the US government to consider itself legally bound by the commitments set out in these letters.[101]

(i) Access and use by US law public authorities for national security purposes (recitals 55-105)

The Commission accepts that the US legal framework has been significantly strengthened since it issued the Communications in 2013. In the Commission's view its analysis shows that US law contains clear limitations on the access and use of personal data transferred under the Privacy Shield for national security purposes as well as oversight and redress mechanisms that provide sufficient safeguards for data to be effectively protected against unlawful interference and the risk of abuse.[102]

- Limitations

The Commission recognises that the President is responsible for ensuring national security while Congress can impose limitations on the way the executive uses this responsibility. As discussed above, PPD-28 is a central legal instrument from the executive that governs access to data for national security purposes.

PPD-28 imposes limitations on signals intelligence operators, has binding force on the Intelligence Community and remains effective upon a change in the US administration.[103] The Commission considers that the ODNI Letter provides "*further assurance*" that the requirements of PPD-28

---

100 Draft Commission Implementing Decision, recital 51.
101 Draft Commission Implementing Decision, recital 53.
102 Draft Commission Implementing Decision, recital 55.
103 Draft Commission Implementing Decision, recital 57.

"*express a general rule of prioritisation of targeted over bulk collection*".[104] The Commission is also reassured that decision-making about what is 'feasible' is subject to policies and procedures that the Intelligence Community must implement under PPD-28.[105]

The Commission considers that bulk data collection is only allowed where targeted collection via the use of discriminants is not possible due to technical or operational considerations.[106] The Commission indicates that PPD-28 limits the use of signals intelligence collected in bulk to a specific list of six national security purposes with a view to protect the privacy and civil liberties of all persons.[107] However the Commission does not acknowledge that these limitations to the use of signals intelligence collected in bulk do not apply to signals intelligence data temporarily acquired to facilitate targeted collection.[108]

In the Commission's view the prioritisation of targeted collection over bulk collection and the limitations around the use of bulk collection reflect the principles of necessity and proportionality. Additionally even when bulk data collection cannot be avoided, any further 'use' of the data through access is strictly limited to specific, legitimate national security purposes. According to the Commission, these reassurances are sufficient for the Privacy Shield to overcome the hurdle set out in *Schrems* concerning US government access to data.[109]

The Commission next assesses the legal bases under FISA for US agencies to access personal data transferred under the Privacy Shield. In the Commission's view the authorisations under FISA to carry out national intelligence activities "*equally restrict public interference to targeted collection and access*".[110] The Commission quotes the PCLOB assessment of Section 702 FISA surveillance that it consists entirely of targeting specific individuals about whom an individualised determination has been made.[111]

The Commission is also reassured by evidence about access requests made through NSLs and FISA and assurances from the US government that the US government is not conducting indiscriminate surveillance, and that the surveillance is targeted and is directed towards a small number of individuals in comparison with the overall flow of data over the internet.[112]

In conclusion, the Commission considers that there are rules in place in the US designed to limit any interference for national security purposes with the fundamental rights of the person whose personal data is transferred under the Privacy Shield Framework to what is strictly necessary to achieve the legitimate objective in question.[113]

---

104 Draft Commission Implementing Decision, recital 59.
105 Draft Commission Implementing Decision, recital 60.
106 Draft Commission Implementing Decision, recital 59.
107 Draft Commission Implementing Decision, recital 61.
108 PPD-28, Footnote 5.
109 *Schrems*, para 93.
110 Draft Commission Implementing Decision, recital 67.
111 Draft Commission Implementing Decision, recital 68.
112 Draft Commission Implementing Decision, recital 69.
113 Draft Commission Implementing Decision, recital 75.

- Effective legal protection - Oversight

The Commission records in extensive detail the various oversight mechanisms within the executive branch (such as civil liberties or privacy officers within US agencies and Inspector Generals), the legislative branch (such as the House and Senate Intelligence and Judiciary Committee in Congress plus requirements on the US government to report to Congress), and the judicial branch (such as the FISC).

- Effective legal protection – Individual redress

The Commission identifies three avenues available under US law for EU individuals who have concerns about the processing of their personal data by the Intelligence Community and lists them as (i) interference under FISA, (ii) unlawful, intentional access to personal data by government officials, and (iii) access to information under the Freedom of Information Act ("**FOIA**").[114]

Individuals can challenge unlawful electronic surveillance under FISA which includes the possibility of bringing a civil cause of action for money damages against the US, to sue US government officials in their personal capacity for money damages, and to challenge the legality of surveillance.[115]

The Commission notes other options for EU individuals to seek legal recourse against government officials under US law such as under the Computer Fraud Abuse Act and Right to Financial Privacy Act.[116]

FOIA also provides a means for EU individuals to seek access to existing federal agency records which could include their personal data (although agencies can withhold information under certain exceptions and such decisions to withhold are themselves subject to challenge). However, FOIA does not in itself provide an avenue for individual recourse against interference with personal data although it can enable individuals to obtain access to relevant information.

But the Commission acknowledges that "*it is equally clear that at least some legal bases that US intelligence authorities may use (e.g. EO 12333) are not covered*" by individual redress mechanisms.[117] Furthermore, courses of action can be limited where an EU individual cannot demonstrate damage (even though damage is not a requirement under EU law for there to be an interference with a fundamental right) and claims brought by non-US persons are inadmissible unless they can show standing which can restrict access to ordinary courts.

The newly created Ombudsperson contributes to ensuring individual redress and independent oversight according to the Commission.[118] The mechanism is devised so that EU individuals can engage with a local body (probably a DPA) in their own country which then helps the individual raise the complaint with the Ombudsperson. In carrying out her functions, the

---

114 Draft Commission Implementing Decision, recital 95.
115 Draft Commission Implementing Decision, recital 96.
116 Draft Commission Implementing Decision, recital 97.
117 Draft Commission Implementing Decision, recital 99.
118 Draft Commission Implementing Decision, recital 101.

Ombudsperson will rely on existing US independent oversight and compliance review mechanisms. Significantly, the Ombudsperson will be independent from the Intelligence Community and is entitled to receive sufficient information to make her own assessment of a matter.[119]

In conclusion, the Commission considers that the US ensures effective legal protection against interferences by its intelligence authorities with the fundamental rights of individuals whose personal data is transferred under the Privacy Shield Framework.

(ii) *Access and use by US public authorities for law enforcement and public interest purposes* (recitals 106–111)

The Commission considers that the US government (through the Department of Justice) has provided assurance on the applicable limitations and safeguards relating to interference with rights for law enforcement purposes and therefore the Commission considers an adequate level of protection has been demonstrated.

The Commission notes that the Fourth Amendment to the US Constitution requires a court-ordered warrant upon a showing of 'probable cause' for searches and seizures by law enforcement agencies, or where a warrant is not necessary, law enforcement agencies must behave reasonably.[120] The restrictions and guarantees set down under the Fourth Amendment reflects, in the Commission's view, the concepts of necessity and proportionality under EU law. However, it is admitted that the protection under the Fourth Amendment does not specifically cover non-US persons although it acts as a restraint on the scope of law enforcement requests to US companies.

Administrative subpoenas are subject to independent judicial review in most instances and US agencies can only seek access to data that is relevant to matters falling within their scope of authority.

(c) Adequate level of protection under the EU-US Privacy Shield (recitals 112-116)

The Commission considers that the findings set out mean that the US ensures an adequate level of protection for personal data transferred under the Privacy Shield Framework. In particular the Commission comments that "*on the basis of the available information about the US legal order, including the representations and assurances from the US government, the Commission considers that any interference by US public authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Privacy Principles, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference*".[121]

---

119 Draft Commission Implementing Decision, recital 104.

120 Draft Commission Implementing Decision, recital 107.

121 Draft Commission Implementing Decision, recital 116.

(d) Action of Data Protection Authorities and information to the Commission (recitals 117-119)

Member States should inform the Commission about relevant action undertaken by DPAs where a DPA handles a complaint from an individual about the compatibility of a Commission adequacy decision. This enables the Commission to effectively monitor the functioning of the Privacy Shield Framework. The Commission also emphasises that acts of the Commission are in principle assumed to be lawful until they are withdrawn, annulled or declared invalid so that a Commission's adequacy decision is binding on all Member States.

(e) Periodic review of adequacy finding (recitals 120–124)

The Commission shall continuously monitor the overall framework created by the Privacy Shield as well as the compliance by US authorities with the assurances contained in the letters that form part of the Privacy Shield Framework.

Additionally representatives from the Commission, the DoC and FTC plus others if relevant will conduct an annual joint review of the Privacy Shield. As part of this review, the Commission will request the DoC to provide information on the referrals the DoC has received from DPAs. After each annual joint review, the Commission will prepare a public report to submit to the European Parliament and Council.

(f) Suspension of the adequacy decision (recitals 125–129)

The Commission reserves the right to suspend the Privacy Shield adequacy decision but will first notify the DoC of its concerns.

6.5 **Assessment against CJEU substantive criteria**

For the purposes of a valid adequacy determination by the Commission, the Privacy Shield Framework must be able to meet the criteria specified by the CJEU and summarised above in Section 5.4. We examine each point below.

(a) **Unrestricted and independent oversight by the DPAs to examine a claim from an individual concerning the protection of his or her right to respect for private and family life and the right to the protection of personal data (Articles 7 and 8 of the Charter). This should be extensively interpreted, in the sense that such competence by the DPAs must have a practical application and be able to lead to the resolution of the matter.**

The Commission's draft adequacy finding clearly stipulates that where a DPA, upon receiving a claim by an EU individual, considers that the individual's personal data transferred to a US organisation are not afforded an adequate level of protection, then the DPA can exercise its powers vis-à-vis the EU data exporter and, if necessary, suspend the data transfer.[122] This stipulation is clear that the DPA can act with complete independence in exercising its functions as required under Article 28 of the Data Protection Directive.

There is no suggestion in the Privacy Shield Framework that the DPA would not be able to investigate a claim under the Privacy Shield. Indeed, there is an obligation on the DoC to work directly with the DPA to deal with compliance and resolve complaints from individuals.

[122] Draft Commission Implementing Decision, recital 44.

Consequently, we do not consider Article 8(3) of the Charter or Article 16(2) of the Treaty of the Functioning of the EU to be interfered with under the Privacy Shield.

Therefore, this criterion is met.

(b) **Ability of the Commission to periodically check whether an adequacy finding is still factually and legally justified.**

The Commission's draft adequacy finding specifically states that the Commission will continuously monitor the functioning of the Privacy Shield Framework with a view to assessing whether the US continues to ensure an adequate level of protection.[123] In addition, the Commission is entitled to suspend, amend or repeal its adequacy decision in cases of systematic failures or where the US public authorities do not comply with their representations and commitments.[124]

Therefore, this criterion is met.

(c) **Any interference must be provided by law, which should be validly enacted and enforceable.**

Certain US laws could potentially interfere with the fundamental rights set out in Articles 7 and 8 of the Charter. However, the ODNI Letter states that US agencies can only access personal data for national security purposes if the agency's request complies with FISA or is made pursuant to a NSL statutory provision. Additionally PPD-28 is clear that signals intelligence can only be collected when based on statute or Presidential authorisation.

Given that any interference must be provided under validly enacted and enforceable laws, it would be essential to ensure that any relevant Executive Orders, proclamations or other Presidential directives are considered validly enacted and maintain their enforceability. The annual review provided for as part of the Privacy Shield provides a regular mechanism to help ensure such authorities remain validly enacted and enforceable.

In connection with accessing data for law enforcement and public interest purposes, federal prosecutors and federal investigative agents can access personal data and thus interfere with fundamental rights but this is only permitted through compulsory legal processes.[125]

This criterion is met to the extent that it is possible to identify validly enacted and enforceable law permitting the interference with fundamental rights.

(d) **Any interference must respect the essence of the rights and freedoms recognised by the Charter, which is underpinned by the principles of democracy and the rule of law.**

The rights and freedoms recognised by the Charter in these circumstances relate to respect for privacy under Article 7, the right to the protection of personal data under Article 8 and the right to an effective remedy under Article 47. Under *Digital Rights Ireland*, the CJEU considered that because the Data Retention Directive

123 Draft Commission Implementing Decision, Article 4(1).
124 Draft Commission Implementing Decision, Article 4(6).
125 Justice Letter, p. 2.

did not permit retention of the content of electronic communications, the impact on the essence of the rights and freedoms was not adverse.

Access to data by US agencies transferred under the Privacy Shield Framework would involve the content of data so that it is not possible to state with absolute certainty that there is no adverse impact on the essence of the rights and freedoms. In the CJEU's view the Derogation Provision was too broad and therefore compromised the essence of the fundamental rights under the Charter. However, while the Derogation Provision is the same in the Privacy Shield Framework, a crucial difference for the purposes of evaluating the effect of the interference with the fundamental rights set out in Articles 7 and 8 of the Charter is that the underlying legal authority for US agencies to rely on the Derogation Provision has profoundly changed over recent years.

PPD-28, which governs the use of signals intelligence data by US agencies, seeks to respect the essence of these rights by stating that:

- All persons have legitimate privacy interests in the handling of their personal information.
- Privacy and civil liberties shall be integral considerations in the planning of US signals intelligence activities.
- Signals intelligence activities must include appropriate safeguards for the personal information of all individuals.
- Bulk data collected cannot be used to silence free speech or unfairly discriminate against individuals.

Additionally, with respect to signals intelligence data, SIGCOM is tasked with ensuring that all the requests submitted to it do not present an unwarranted risk to privacy and civil liberties. Consequently, we do not consider the Privacy Shield Framework to fatally threaten the essence of fundamental rights given that the current US legal framework also aims to protect similar rights.

Although we are not aware of similar requirements on US agencies when using non-signals intelligence data we note that US agencies are accountable both to Congress and to the courts for their use of personal data. But the essence of the rights and freedoms recognised by the Charter would be in jeopardy if, for instance, individuals were never told that their personal data has been used for national security, law enforcement or public interest purposes under any circumstances.

On balance, we consider it likely that this criterion is met, particularly taking into account the principles of democracy and the rule of law which underpin the application of the US legal framework.

(e) **Any interference must be proportionate so that the law must be appropriate to attain its legitimate objectives.**

Under CJEU case law, the "*principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives*".[126] Additionally, 'proportionality'

[126] *Digital Rights Ireland*, para 46.

(along with 'necessity') was one of the essential guarantees identified by the Article 29 Working Party as necessary to justify access to personal data. The Privacy Shield Framework proposed by the Commission seeks to argue that the US ensures an adequate level of protection for personal data transferred under the Privacy Shield Framework from the EU to self-certified organisations in the US. Part of the Privacy Shield Framework recognises that personal data will be accessed by US agencies for national security, law enforcement and public interest purposes. The question is whether the interference with fundamental rights set out in the Privacy Shield Framework as agreed by the Commission with the US government is proportionate.

It is important to emphasise that the CJEU has ruled that any discretion by an EU institution is reduced in view of the important role played by Articles 7 and 8.[127] However, it is in the commercial and political interests of both the EU and the US for the respective governments to agree a successor to the Safe Harbor Framework. In the light of the vital importance of the digital economy, failure to agree on a suitable successor to the Safe Harbor Framework has serious implications for on-going trade between the two blocs and their respective economies. The Privacy Shield may be considered to be appropriate for attaining the objective pursued. Likewise, both the EU (and their Member States) and the US have valid and pressing reasons to access and use personal data for national security, law enforcement and public interest purposes.

The concern is whether the access and use by US agencies to the Privacy Shield data could be disproportionate and therefore cast doubt on the proportionality of any interference with fundamental rights. But the Privacy Shield documents set out a number of arguments why access and use are not disproportionate:

- Signals intelligence activities must be tailored as feasible.[128]
- Use of signals intelligence collected as bulk data is restricted to six specific purposes which bear similarities with the scope for exemptions and restrictions under Article 13 of the Data Protection Directive.[129]
- The Commission considers that targeted collection of signals intelligence is prioritised over bulk collection.[130]
- FISA authorisations restrict interference and encourage targeted collection and access.[131]
- Evidence provided by the US government concerning access requests using NSLs and FISA indicate that the US government is not conducting indiscriminate surveillance.[132]
- Any subpoena issued by law enforcement agencies or federal agents for public interest purposes cannot be overbroad, oppressive or burdensome.

---

127 *Digital Rights Ireland*, para 48.

128 ODNI Letter, p. 3.

129 PPD-28, p. 3-4; Article 13 of the Data Protection Directive enables Member States to restrict the scope of certain obligations and rights provided for in the Directive when such a restriction constitutes a necessary measure to safeguards, inter alia, national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions.

130 Draft Commission Implementing Decision, recital 63.

131 Draft Commission Implementing Decision, recital 67.

132 Draft Commission Implementing Decision, recital 69.

- Guidance from the Attorney General requires the FBI to use the least intrusive investigative methods feasible.

To the extent that there is an exception to the six purposes for using signals intelligence data collected in bulk, the exception only permits use on a temporary basis and for a specific purpose – to facilitate targeted collection. Consequently, due to these limitations around such use, we do not see this exception as disproportionate.

Whereas in *Digital Rights Ireland*, the CJEU found that there were no restricting rules preventing the interference with fundamental rights and the requirements of the Data Retention Directive affected all users of electronic communications in the EU regardless of whether they were linked to a serious crime, under the Privacy Shield Framework access by US agencies is subject to a host of rules, laws, guidelines and court authorisations, and access is targeted and tailored so as not to affect all individuals whose personal data is transferred under the Privacy Shield.

In view of the specific circumstances and conditions under which US intelligence activities may lawfully take place, we consider it likely that this criterion is met.

(f) **Any interference must be limited to what is strictly necessary.**

This criterion is closely linked with the requirement for proportionality above and meeting an objective of general interest below. Any limitations to fundamental rights must only be those that are strictly necessary. Similarly, 'necessity' (along with 'proportionality') was one of the essential guarantees identified by the Article 29 Working Party as necessary to justify access to personal data. In *Digital Rights Ireland*, the CJEU commented that the fight against serious crime was of the utmost importance.[133] But even though this was an objective of general interest, it did not justify the broad retention requirements contained in the Data Retention Directive being considered to be necessary for the purpose of that fight.

As explained in relation to the proportionality arguments referred to above, US law contains a number of strict and detailed rules requiring targeted and tailored access to data that indicates that any interference with Articles 7 and 8 would be limited to what is strictly necessary to achieve the legitimate objectives of national security, law enforcement and public interest.

Therefore, this criterion is met.

(g) **Any interference must genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.**

In *Digital Rights Ireland*, the CJEU recognised that the fight against international terrorism in order to maintain international peace and security was an objective of general interest.[134] Consequently the CJEU was content to state that the "*retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest*".[135] Consequently the CJEU did not rule

133 *Digital Rights Ireland*, para 51.
134 *Digital Rights Ireland*, para 42.
135 *Digital Rights Ireland*, para 44.

that the Data Retention Directive was invalid because it failed to meet this criterion. In the eyes of the CJEU, the Data Retention Directive did meet this criterion. It follows that interference with fundamental rights to meet objectives of national security, law enforcement and public interest by the US agencies is a genuine objective that would be recognised by the EU.

Therefore, this criterion is met.

(h) **The scope of the interference must be expressed in clear and precise rules.**

The requirement according to the CJEU is for EU law to lay out clear and precise rules governing the scope and application of a measure that interferes with fundamental rights. This was also one of the essential guarantees identified by the Article 29 Working Party. The scope of the interference with Articles 8 and 7 with respect to Privacy Shield personal data is comprehensively covered in the Privacy Shield documents. In particular, the ODNI Letter sets out a range of safeguards and limitations applicable to US national security authorities, including collection limitations, retention and dissemination limitations, and compliance and oversight mechanisms. Likewise, the Justice Letter describes a number of safeguards and limitations on US government access to data for law enforcement and public interest purposes.

Therefore, while we consider that the expression of the scope of interference could be clarified further in certain places and even greater precision could be helpful, we do not see these deficiencies as fatal given the degree of detail with which intelligence activities and government access to data are regulated.

On the basis of the various safeguards and limitations described in the Privacy Shield documents, we consider it likely that this criterion is met.

(i) **There are minimum safeguards to ensure sufficient guarantees to protect the personal data against abuse and unlawful access and use.**

The CJEU has stated that the need for safeguards is all the greater where personal data is subjected to automated processing and where there is a significant risk of unlawful access to that data.[136]

Under PPD-28, US agencies must ensure that signals intelligence activities include appropriate safeguards for the personal information of individuals. Additionally, information collected under Section 702 of FISA may only be reviewed by trained intelligence personnel who can only use the data to identify foreign intelligence information or evidence of a crime.

Safeguards are also provided through the complaint and oversight mechanisms set out in the Privacy Shield. For instance, the framing of intelligence priorities under NIPF and the involvement of SIGCOM in checking that all requests for signals intelligence conforms with NIPF. Additionally, safeguards are implemented so that decisions about what is feasible and practical under PPD-28 are not left to the discretion of a single individual but are set out in policies to which US agencies are accountable for complying with.

On the basis of the various safeguards and limitations described in the Privacy Shield documents, we consider it likely that this criterion is met.

[136] *Schrems*, para 91.

(j) **There is proper accountability for third country public authorities accessing the data.**

It was not evident under the Safe Harbor Framework how US agencies were held accountable for accessing data lawfully. However, the Privacy Shield Framework goes into substantial detail on the different layers of oversight and accountability.

For instance, collection of data under Section 702 of FISA is subject to oversight from within the Executive Branch as well as Congress. Likewise, oversight is provided over US agencies involved in foreign intelligence and signals intelligence data collection on a number of levels. While a number of these oversight levels could be said to lack objective independence (for instance, oversight personnel within the Intelligence Community or the ODNI's own Civil Liberties and Privacy Office), there are several examples of oversight levels operating in the executive, legislative and judicial branches. Indeed certain accountability mechanisms such as the FISC have been recently strengthened so that there is greater accountability for privacy matters.

Complaints about interference with fundamental rights involving signals intelligence data will be dealt with by the Ombudsperson who has power to work together with other US government officials to ensure that complaints from individuals are processed and resolved in accordance with applicable laws and policies.[137] The Ombudsperson reports back to an individual that a complaint has been properly investigated and that US law etc. has been complied with or that any non-compliance has been remedied.[138] The Ombudsperson is not permitted to go into detail about the remedy applied but the implication is that the Ombudsperson will help to keep US agencies accountable for compliance with the rules when accessing data.

The new focus on transparency as a result of the USA FREEDOM Act will also improve accountability by US agencies since there is regular reporting about their activities.

Therefore, this criterion is met.

(k) **There are objective criteria determining the limits of access by public authorities to the data and its subsequent use for specific and strictly restricted purposes.**

All US statutes and constitutional rules authorising information gathering by the government, as well as PPD-28 (for signals intelligence) sets out limits of access to and use of data by US agencies.[139] National security intelligence gathering criteria are reviewed annually by the Assistant to the President and the National Security Advisor in consultation with the DNI. Any amendments to the criteria are then presented to the President for confirmation.

Under Section 702 of FISA, intelligence personnel can only use data collected to identify foreign intelligence information or evidence of a crime, and individuals can be held personally liable for violating these restrictions.

Therefore, this criterion is met.

---

137 Ombudsperson Letter, p. 2.

138 Ombudsperson Letter, p. 4.

139 Although PPD-28 only refers to 'use' of the data, by permitting certain uses, this is also indicating that the data can be accessed for such use.

(l) **Individuals must have a right to pursue effective legal remedies before an independent and impartial tribunal previously established by law, as enshrined in Article 47 of the Charter.**

Where an individual's rights and freedoms under the Charter are violated, they have a right to an effective remedy before a tribunal which permits a fair and public hearing by an independent and impartial tribunal. The Article 29 Working Party likewise identified effective remedies available to individuals to ensure anyone is able to defend their rights as an essential guarantee. Under the Privacy Shield Framework, an individual can pursue legal remedies in the following ways:

- Complaints about lack of compliance with the Privacy Shield Principles by organisations can be first brought to the organisation – including through the DoC following a referral by a DPA – that is then required to respond within 45 days,[140] or they can be sent to an independent dispute resolution body, including an authority designated by a panel of DPAs where organisations have committed to such cooperation. Ultimately the DoC and the FTC can help investigate and resolve the complaint. If all else fails, there is an arbitration last resort which an individual can turn to. This is without prejudice of other commercial remedies that may be available, including private claims through US courts.

- Relief in connection with interferences with fundamental rights for the purposes of national security may be sought through US courts. In particular, individuals may bring a civil claim for damages when information about them has been unlawfully and wilfully used or disclosed. Individuals subjected to unlawful electronic surveillance may sue US government officials for damages and challenge the legality of surveillance. EU-based individuals and citizens may also seek legal redress under US laws including the Computer Fraud and Abuse Act, Electronic Communications Privacy Act and Right to Financial Privacy Act where applicable.

- Complaints about interference with fundamental rights for the purposes of national security may additionally be dealt with by the Ombudsperson who can report on the compliance or lack of compliance by the US agency. Importantly, the Ombudsperson is established to be wholly independent from the US agencies, although as part of the practical operation of this function, it will be necessary to ensure that the Ombudsperson is able to direct the application of an effective remedy.

- Complaints about interference with fundamental rights for the purposes of law enforcement and the public interest are effected by the ability to file motions to challenge subpoenas.

In summary, individuals can primarily seek effective legal remedies through the US courts by relying on a number of US laws. However, there is acknowledgement that there are legal bases available to US agencies that are not clearly covered by a method of obtaining legal remedies. Therefore, it appears that the role of the Ombudsperson is to fill any gaps. Consequently, it will be crucial to demonstrate that, in the Ombudsperson, individuals have a right to pursue effective legal remedies. This is an essential part of the operation of the

[140] Although the reference in Annex II, para 11 (d) only gives consumers this right, we expect that in reality the right is for all individuals including non-consumers.

Privacy Shield Framework which needs to be properly implemented in order to tackle any claims that the scheme does not fully protect the rights under Article 47.

Given the various legal remedies that may be sought through the US courts and on that basis that the practical implementation of the Ombudsperson mechanism may provide an effective supplemental avenue to pursue legal remedies, we consider it likely that this criterion is met.

7. CONCLUSION

We have considered the adequacy of the Privacy Shield Framework by reference to the jurisprudence of the CJEU. The CJEU has made it clear that for any adequacy determination of a third country by the Commission, the third country must meet certain criteria that we have identified in section 5 and examined the Privacy Shield Framework against in section 6.

In our concluding remarks we consider it important to remember that the mere transfer of personal data from the EU to the US is not necessarily an infringement of Articles 7, 8 and 47 of the Charter. Whilst in *Digital Rights Ireland*, the mere retention of all personal data was an infringement of Articles 7 and 8, this was because there were no clear and precise rules governing the extent of the interference into fundamental rights and the Data Retention Directive did not provide for sufficient safeguards to ensure the effective protection of data against the risk of abuse and against unlawful access and use. The Safe Harbor Framework also suffered from certain deficiencies since the Safe Harbor Decision did not demonstrate that the Commission had examined US laws with sufficient rigour with respect to potential interferences with fundamental rights.

In the case of the Privacy Shield Framework, the potential for infringement of fundamental rights arises when US agencies seek to access the personal data under the Derogation Provision. But the Privacy Shield Framework differs significantly from the Safe Harbor Framework. The Privacy Shield Framework describes the rules governing access to data and therefore the extent of interference into fundamental rights and explains the safeguards to ensure effective protection of data against possible abuse and unlawful access. The Privacy Shield Principles should be read in conjunction with the assurances concerning limitations and safeguards under US law, so that it can be concluded that it is not the case that the fundamental rights of large numbers of individuals are likely to be infringed simply because their personal data is transferred under the Privacy Shield Framework.

We recognise the considerable changes that have taken place in US domestic law since the Snowden revelations in June 2013 about surveillance practices by the US (and other countries). In particular, the introduction of PPD-28, the amendments to FISA, the strengthened role of FISC and other transparency requirements demonstrate the substantial political effort by the US government to strengthen privacy protections for all individuals. Furthermore, there is greater emphasis on targeted and tailored access by US agencies to data and, in particular, data collected in bulk can only be used for six specific national security purposes. These changes underline the approach that the interferences with fundamental rights are necessary, proportionate and only as strictly necessary to attain the objectives of national security, law enforcement and the public interest.

EU and US privacy law frameworks are not identical and therefore any direct comparison runs the risk of over-simplification and not comparing like for like. For instance, unlike each of the EU Member States, the US does not have a single data protection agency. But the involvement of the FTC, DoT, DoC as well as the Privacy and Civil Liberties Oversight Board provides accountability, oversight and enforcement functions and the Privacy Shield Framework additionally allows for further oversight through arbitration and the Ombudsperson as well as input from DPAs.

Whilst we accept that certain aspects of the Privacy Shield Framework would benefit from greater clarity, precision and accessibility, we are satisfied that these potential weaknesses do not affect the overall effect of the Privacy Shield Framework and the level of privacy and data protection that it affords.

Ultimately, the level of adequacy of the Privacy Shield Framework will be determined by its day-to-day operation and the ability of participants to meet its requirements in an effective and visible manner. In our view, all of the Commission's recommendations for improvements have been satisfactorily addressed (see Appendix II – Measures in response to European Commission's Recommendations), but in reality the true level of data protection afforded by the Privacy Shield Framework will only be demonstrated by its functioning and the practices of its participants.

The key question this report sets out to answer is: ***Does the Privacy Shield Framework meet the criteria for adequacy under Article 25(6) of the Data Protection Directive as interpreted by the CJEU?*** Our assessment indicates that the Privacy Shield Framework does substantially meet the criteria laid out.

Therefore we conclude that, on the basis of our detailed assessment set out in this report, **the Privacy Shield Framework provides an 'essentially equivalent' level of protection for personal data transferred from the EU to the US.**

31 March 2016

APPENDIX I – DEFINED TERMS

Term	Definition
ADR	Alternative Dispute Resolution
Article 29 Working Party	A Working Party set up under Article 29 of the Data Protection Directive and comprised of representatives of the national data protection authorities of each of the EU Member States, the European Data Protection Supervisor and the European Commission
BCR	Binding Corporate Rules
Bot	Opinion of Advocate General Bot, delivered on 23 September 2015, Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Commission	European Commission
Communications	Two communications from the Commission to the European Parliament and the Council on 27 November 2013: • "*On the functioning of the Safe Harbor from the Perspective of EU citizens and Companies Established in the EU*" COM(2013) 847 final; and • "*Rebuilding Trust in EU-US data flows*" COM(2013) 846 final
Council	European Council
Data Protection Directive	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 the free movement of such data
Data Retention Directive	Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
Derogation Provision	Wording in the fourth paragraph of Annex I of the Safe Harbor Decision indicating that adherence to the Safe Harbor Privacy Principles may be limited in certain circumstances e.g. to the extent necessary to meet national security, public interest, or law enforcement requirements
Digital Rights Ireland	*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, and others*, 8 April 2014, CJEU, C-293/12
DNI	US Director of National Intelligence
DoC	US Department of Commerce
DoT	US Department of Transportation
DPA	European Data Protection Authority
EEA	European Economic Area (consisting of the EU Member States together with Iceland, Liechtenstein and Norway)
EO 12333	US Executive Order 12333

EU	European Union
EU Member States	Member states of the European Union
FISA	US Foreign Intelligence Surveillance Act
FISC	US Foreign Intelligence Surveillance Court
FOIA	US Freedom of Information Act
FTC	US Federal Trade Commission
GDPR	EU General Data Protection Regulation, which was agreed by the EU's legislative institutions in December 2015 and is set to replace the regime created by the Data Protection Directive in 2018.
Irish Commissioner	Irish Data Protection Commissioner
Irish High Court	High Court of Ireland
Justice Letter	Letter from the US Department of Justice dated 19 February 2016 and appearing as Annex III to the Privacy Shield Decision
NIPF	US National Intelligence Priorities Framework
NSA	US National Security Agency
NSL	US National Security Letter
ODNI	US Office of the Director of National Intelligence
ODNI Letter	Letter from the ODNI dated 22 February 2016 and appearing as Annex VI to the Privacy Shield Decision
Ombudsperson	The Privacy Shield Ombudsperson created by the Privacy Shield Framework
Ombudsperson Letter	Letter from US Secretary of State John Kerry dated 22 February 2016 and appearing as Annex III to the Privacy Shield Decision
PCLOB	Privacy and Civil Liberties Oversight Board
PPD-28	Presidential Policy Directive 28, issued by President Obama in January 2014
Privacy Shield Data	EU personal data transferred under the Privacy Shield Framework
Privacy Shield Decision	Draft Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield
Privacy Shield Framework	The EU-U.S. Privacy Shield framework
Privacy Shield Principles	The seven Principles and 13 Supplemental Principles of the Privacy Shield Framework set out in Annex II of the Privacy Shield Decision
Safe Harbor Decision	Commission Decision of 26 July 2000 pursuant to Data Protection Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce
Safe Harbor	The Safe Harbor framework agreed by the US Department of Commerce

Framework	and the European Commission in 2000
Safe Harbor Privacy Principles	The seven Principles of the Safe Harbor Framework
SCC	Standard Contractual Clauses approved by the European Commission
Schrems	*Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, CJEU, Case C-362/14
SIGCOM	US National Signals Intelligence Committee
US	United States of America

APPENDIX II – MEASURES IN RESPONSE TO EUROPEAN COMMISSION'S RECOMMENDATIONS

Recommendation	Measure
Transparency	
Scheme members' privacy policies should be published on their websites in clear and conspicuous language.	The Notice principle requires participants to provide a notice to individuals containing thirteen specified details, in clear and conspicuous language, at the time the individual is first asked to provide personal information or as soon as is practicable thereafter.[141]
Scheme members' privacy policies should link to a list of all current members of the scheme maintained on the DoC website.	The Notice principle requires participants to provide a link to, or a web address for, the list of all current Privacy Shield participants maintained by the DoC.[142]
Scheme members should disclose the data protection provisions of contracts with any third party providers who process data transferred to the US under the scheme.	The Accountability for Onward Transfer principle requires participants to provide a summary or copy of the relevant data protection provisions of their contracts with service providers to the DoC on request.[143]
The DoC should clearly identify companies which are no longer members of the scheme on its website. Those which cease to be members should still protect data received under the Safe Harbor Framework.	The DoC will maintain and make available to the public a record of organisations that had been Privacy Shield certified but have been removed.[144] The DoC will identify the reason for the removal[145] and provide a clear warning that these organisations are not participants in the Privacy Shield.[146] The Data Integrity and Purpose Limitation principle requires participants to adhere to the Privacy Shield Principles for as long as they retain information transferred under the Privacy Shield, regardless of whether the company withdraws from the framework.[147] A prominent reminder of this will be displayed on the Privacy Shield website.[148] The DoC will send questionnaires to organisations whose self-certification has lapsed or who have voluntarily withdrawn from the Privacy Shield to verify how the organisation will continue to protect Privacy Shield data.[149]

141 Annex II, Section II, para 1 (a).
142 Annex II, Section II, para 1 (a) (i).
143 Annex II, Section II, para 3 (b).
144 Annex II, Section I, para 4.
145 Annex I, page 5.
146 Annex II, Section I, para 4.
147 Annex II, Section I, para 3.
148 Annex I, page 5.
149 Annex I, page 6.

Redress	
Scheme members' privacy policies should contain a link to an alternative dispute resolution ("**ADR**") provider or the EU Data Protection Panel.	The Notice principle requires participants to include details of (i) any relevant establishment in the EU that can respond to inquiries or complaints[150], (ii) the independent dispute resolution body designated to address complaints[151], (iii) a hyperlink to the complaint submission form of that dispute resolution body[152], and (iv) the possibility for EU individuals to invoke additional binding arbitration.[153]
ADR should be readily available and affordable to individuals.	The Recourse, Enforcement and Liability principle requires participants to subscribe to an independent recourse mechanism to deal with any complaints from EU individuals that the organisation is unable to resolve itself. The recourse mechanism must be impartial, readily available and free for the individual.[154] Additionally, an individual may complain to their local EU DPA about a Privacy Shield organisation's processing of their personal data and the DPA may then raise the matter with the DoC. The DoC and FTC will investigate and resolve complaints forwarded by a DPA.[155] Where there are claims that are still not satisfactorily resolved, an individual may resort to an arbitration option with arbitrators appointed to sit on a Privacy Shield Panel. The arbitrators can determine whether an organisation has violated its obligations under the Principles but cannot consider questions relating to the Derogation Provision or any concern about the adequacy of the Privacy Shield Framework. Any ruling from the Privacy Shield Panel can impose individual-specific, non-monetary equitable relief to remedy non-compliance.[156]
The DoC should monitor more systematically the transparency and accessibility of information ADR providers set out regarding how they deal with complaints.	Both Privacy Shield organisations and the independent dispute resolution body must respond promptly to requests from the DoC.[157] Independent dispute resolution providers are required to (a) include six specified details on their websites;[158] and (b) publish an annual report detailing complaints received and how they have been dealt with.[159] Independent dispute resolution providers must respond promptly to requests from the DoC.[160]

150 Annex II, Section II, para 1 (a) (v).
151 Annex II, Section II, para 1 (a) (ix).
152 Annex I, page 6.
153 Annex II, Section II, para 1 (a) (xi).
154 Annex II, Section II, para 7 (a) (i).
155 Annex I, page 8 and 9.
156 Annex II (Annex I thereof).
157 Annex II, Section II, para 7 (b).
158 Annex II, Section III, para 11 (d) (ii).
159 Annex II, Section III, para 11 (d) (iii).
160 Annex II, Section II, para 7 (b).

Enforcement	
A certain percentage of companies certifying or recertifying under the Safe Harbor Framework should be subject to ex-officio investigations to determine whether they are complying with their privacy policies.	The DoC will monitor effective compliance with the Privacy Shield Framework on an on-going basis, including through sending detailed questionnaires to participating organisations. The DoC will take follow-up action where the organisation does not respond satisfactorily to DoC inquiries or where there is credible evidence that the organisation does not comply with the Privacy Shield Principles.[161] The DoC has doubled the number of staff responsible for administering and supervising the Privacy Shield Framework, and committed to continue dedicating appropriate resources to ensure its effective monitoring and administration.[162] The FTC will investigate possible violations of the Privacy Shield Framework of its own initiative where appropriate.[163] Organisations must retain records demonstrating their implementation of the Privacy Shield Principles as these could be required in the course of an investigation and could ultimately be made public.[164]
Any finding of non-compliance should result in a follow-up investigation after one year.	The FTC has highlighted that in the three enforcement actions it brought for alleged violations of Safe Harbor Privacy Principles, it imposed consent orders requiring the relevant participants to submit to on-going and independent assessments of their privacy programmes for a twenty-year period.[165] The FTC has committed to continue monitoring such orders.[166]
DPAs should be informed where there are doubts about a company's compliance or a pending complaint.	The Privacy Shield Framework contains an obligation on the DoC to work directly with the DPAs to deal with compliance and resolve complaints from individuals.[167]
False claims of Safe Harbor adherence should continue to be investigated.	The DoC will be more proactive in searching for and addressing false claims that organisations maintain Privacy Shield status which will include spot-checks of the privacy notices of previously certified organisations, conducting internet searches to identify where images of the Privacy Shield certification mark are being displayed to check whether such use is valid, as well as reviewing and addressing complaints about false claims of participation promptly.[168]

161 Annex I, page 8.
162 Annex I, page 8.
163 Annex IV, page 7.
164 Annex II, Section III, para 7 (e).
165 Annex IV, page 5.
166 Annex IV, page 2.
167 Annex I, page 8.
168 Annex I, page 7.

Access by US authorities	
Scheme members' privacy policies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbor Framework. Companies should be encouraged to indicate when they apply exceptions to the Safe Harbor Privacy Principles in order to meet national security, public interest or law enforcement requirements.	The USA FREEDOM Act allows participants to publish transparency reports setting out the number of FISA orders, directives or NSLs they receive from the US government and the limited number of customers whose records have been sought.[169] The Notice principle requires participants to include in their privacy policies the fact that they are required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.[170] A new FAQ in the Privacy Shield Principles allows Privacy Shield organisations to voluntarily provide transparency by issuing periodic transparency reports on the number of requests for personal data that they receive from public authorities.[171]
The national security exception should be used only when strictly necessary or proportionate.	The USA FREEDOM Act: (a) prohibits the collection in bulk of records where such collection is based on Section 402 FISA (which permitted the collection of internet metadata), Section 501 FISA (which permitted the collection of phone metadata) or NSLs[172]; and (b) increases transparency over surveillance and national security activities by US agencies.[173] Presidential Policy Directive 28 ("**PPD-28**"): - sets out further principles and restrictions on the use of signals intelligence data for non-US persons as well as US citizens; - makes clear that signals intelligence can only be collected when based on statute or Presidential authorisation; and - has binding force on the Intelligence Community and remains effective upon a change in the US administration.[174] The ODNI Letter contains assurances that PPD-28 and its associated processes and procedures enabling the collection, retention and dissemination of foreign intelligence: (a) provide important privacy protections for all individuals, regardless of nationality[175]; and (b) directs US agencies to prioritise targeted signals intelligence rather than bulk signals intelligence. The Justice Letter provides an overview of the primary investigative tools used to obtain data held by Privacy Shield organisations, including

169 Annex VI, p. 14.
170 Annex II, Section II, para 1 (xii).
171 Annex II, Section III, para 16 – Access Requests by Public Authorities.
172 Draft Commission Implementing Decision, recital 66.
173 Annex VI, p. 14.
174 Draft Commission Implementing Decision, recital 57.
175 Annex VI, p.9.

	their limitations and organisations' rights of appeal.[176] A new Privacy Shield Ombudsperson is responsible for ensuring that EU individuals who submit complaints to their DPA about US signals intelligence receive an appropriate response confirming whether the complaint has been properly investigated and whether US law and related directives, orders and policies providing limitations and safeguards have been complied with.[177]

176 Annex VII.
177 Annex III.

APPENDIX III – PRACTICAL COMPLIANCE REQUIREMENTS UNDER THE PRIVACY SHIELD PRIVACY PRINCIPLES

Organisations wishing to participate in the Privacy Shield will need to comply with the following requirements:

Notice

- Publish a privacy policy containing thirteen specified details, including:
    - any relevant establishment in the EU that can respond to inquiries or complaints about EU personal data transferred under the Privacy Shield Framework ("**Privacy Shield Data**");
    - the independent dispute resolution body designated to address complaints;
    - a hyperlink to the complaint submission form of that dispute resolution body;
    - the possibility, under certain circumstances, for EU individuals to invoke additional binding arbitration; and
    - the possibility that the organisation may be held liable for unlawful transfer of Privacy Shield Data to third parties.

Choice

- Provide a mechanism for individuals to opt out of having their Privacy Shield Data disclosed to a third party or used for a materially different purpose than that for which it was provided (not applicable to disclosures to third-party service providers that use Privacy Shield Data solely under the instructions of the participating organisation (i.e. data processors).
- Obtain affirmative express consent from individuals prior to sharing sensitive Privacy Shield Data with a third party or using it for a purpose other than for which it was initially collected.

Accountability for Onward Transfer

- If providing Privacy Shield Data to any third party that will use it for its own purposes (i.e. data controllers), enter into a contract providing that Privacy Shield Data may only be processed for limited and specified purposes consistent with individual consent, and that the recipient will provide the same level of protection as the Privacy Shield Principles.
- If providing Privacy Shield Data to any third party service provider:
    - either (i) ascertain that the service provider is subject to an EU adequacy finding (including being a Privacy Shield member) or (ii) enter into a written agreement requiring the service provider to provide the same level of protection as the Privacy Shield Principles;
    - only transfer data for limited and specified purposes;
    - “take reasonable and appropriate steps to ensure that the [service provider] effectively processes the personal information transferred in a manner consistent with the organization’s obligations under the Principles”; and
    - if the organisation has entered into a written agreement with a service provider, provide a summary or copy of the relevant privacy provisions of the contract with the service provider to the DoC upon request.

Security

- Take reasonable and appropriate measures to protect Privacy Shield Data from loss, misuse and unauthorised access, disclosure, alteration, and destruction, taking into due account the nature of the Privacy Shield Data and the risks involved in its processing.

Data Integrity and Purpose Limitation

- Limit processing to the purposes for which Privacy Shield Data was originally collected or has been subsequently authorised.
- Take reasonable steps to ensure that Privacy Shield Data is reliable for its intended use, accurate, complete, and current.
- Adhere to the Privacy Shield Principles for as long as the participating organisation retains Privacy Shield Data, regardless of whether it withdraws from the framework.

Access

- Provide a mechanism by which individuals may request Privacy Shield Data related to them to be corrected, amended, or deleted.
- Provide a mechanism by which individuals may obtain confirmation of whether an organization is processing Privacy Shield Data related to them.

Recourse, Enforcement and Liability

- Respond to complaints from EU individuals relating to Privacy Shield Data within 45 days.
- Register with a third-party ADR provider to assess any complaints from EU individuals relating to Privacy Shield Data that the organisation is unable to resolve. This arbitrator must:
    - be offered at no cost to the individual; and
    - be empowered to impose damages “where the applicable law or private-sector initiatives so provide”.
- Respond promptly to inquiries and requests by the DoC, including those referred to the DoC by European DPAs.
- Arbitrate any residual claims from EU individuals that the organisation has violated its obligations under the Privacy Shield Principles.
- If subject to an FTC or court order based on non-compliance, make public “any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC” to the extent consistent with confidentiality requirements.
- Verify compliance with the Privacy Shield.
- Retain records of the implementation of Privacy Shield privacy practices and make them available in the course of an investigation (these may later become public).
- Either:
    - Affirm compliance to the Department of Commerce on an annual basis, even if the organisation withdraws from the framework;
    - Return or delete all Privacy Shield Data; or
    - Affirm that Privacy Shield Data will be adequately protected by another authorised means (e.g. EU standard contractual clauses).