From the Office of the Director General
John Higgins CBE

DIGITALEUROPE

BRUSSELS, 11 April 2016

Mr Ard Van der Steur
Minister of Security and Justice
Dutch Ministry of Security and Justice
Turfmarkt 147
2511 DP Den Haag – Netherlands

RE: Future Adoption of the draft EU-US Privacy Shield Adequacy Decision (Article 31 Committee)

Dear Minister Van der Steur,

As the voice of the digital technology sector in Europe, DIGITALEUROPE has long supported the ambitions of the EU institutions to restore trust in transatlantic data flows. We welcome the publication of the draft EU-US Privacy Shield Adequacy Decision and **strongly support its prompt adoption**, which is essential to re-establishing a sustainable path for data transfers between the EU and the US.

The EU and US are each other's most important markets. The political, cultural and economic ties between these partners means that the transfer of personal data across the Atlantic is inevitable. A disruption in transatlantic data flows could reduce EU GDP by up to 1.3% and lead to a 6.7% drop in EU services exports to the US.[1] At a time of continued economic recovery in Europe, such a negative economic shock must be avoided.

The invalidation of the Safe Harbour framework by the Court of Justice of the EU (CJEU) created an unprecedented state of legal uncertainty for European and US businesses of all sizes, particularly SMEs, which made up approximately 60% of Safe Harbour certified companies. Beyond annulling the validity of transfers under this widely used legal instrument, this Judgement has caused regulators to cast doubt on the use of alternative transfer mechanisms such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) in the EU-US context calling into question the viability of all transatlantic data transfers. **This legal uncertainty has to stop.**

We applaud the efforts of the European Commission to ensure that the new transfer tool is a solid mechanism that can withstand any test, including a possible Court challenge. We believe that the EU-US Privacy Shield achieves this goal and is an instrument that can reinstall much needed legal certainty. We encourage policy makers to review the recent legal study published by Hogan Lovells[2], particularly Section 6.5 (See Annex), which sets out arguments as to why the Privacy Shield meets the criteria of the Schrems Decision[3]. We also take note of the yearly review mechanism and suspension clause, as well as the reinforced and institutionalised collaboration between the EU and the US authorities. These will allow for any necessary adjustments in the future.

The new framework is also **more demanding on companies**, placing strict rules for the onward transfer of data by requiring a contract for data sharing with any third party. Companies will also be required to respond to user complaints within 45 days. Such requirements go beyond the requirements found in the new General Data Protection Regulation (GDPR). While such obligations will be difficult for companies, **DIGITALEUROPE members are ready to meet the compliance challenge**. They are ready to do this not only because it is necessary from a legal point of view, but because it is good for data protection and strong data protection is critical to rebuilding transatlantic trust.

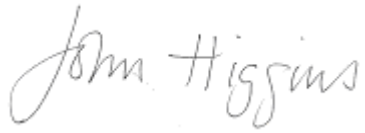
1 European Centre for International Political Economy (ECIPE), "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce", March 2013 (Link).
2 Hogan Lovells LLP, "Legal Analysis of the EU-U.S. Privacy Shield: An adequacy assessment by reference to the jurisprudence of the Court of the Justice of the European Union", 31 March 2016 (Link).
3 Case C-362/14 (Maximillian Schrems v Data Protection Commissioner)

Data transfers are an essential part of our interconnected world and we need strong legal instruments that companies can confidently rely on to ensure that such transfers respect legal requirements and include the necessary safeguards to maintain a high level of protection of personal data. The legal instruments that European data protection regulators and decision makers have put in place, such as the SCCs, BCRs and now the Privacy Shield are in place to ensure this. **Our members take compliance with these instruments very seriously** and are deeply committed to abiding by the legal requirements that ensure a high level of data protection when transferring data across borders.

However, after months of uncertainty, it is time to restore trust and legal certainty for citizens and for the thousands of European and American businesses, both large and small, that depend on transatlantic data transfers. We cannot build a successful Digital Single Market without allowing companies to scale up and reach global markets.

DIGITALEUROPE thus urges all decision makers to ensure a **swift adoption of the Privacy Shield and reaffirm the use of the alternative transfer mechanisms.**

Sincerely,



John Higgins
Director General
DIGITALEUROPE

CC:

Mr Wolfgang Brandstetter, Federal Minister, Austrian Federal Ministry of Justice

Mr Koen Geens, Minister of Justice, Belgian Ministry of Justice

Ms Ekaterina Zaharieva, Minister of Justice, Bulgarian Ministry of Justice

Mr Ante Šprlje, Minister of Justice, Croatian Ministry of Justice

Mr Ionas Nicolaou, Minister of Justice and Public Order, Cypriot Ministry of Justice and Public Order

JUDr. Robert Pelikán, Minister of Justice, Czech Ministry of Justice

Mr Søren Pind, Minister of Justice, Danish Ministry of Justice

Mr Urmas Reinsalu, Minister of Justice, Estonian Ministry of Justice

Mr Jari Lindström, Minister of Justice and Employment, Finnish Ministry of Justice

Mr Jean-Jacques Urvoas, Minister of Justice, French Ministry of Justice

Dr Thomas de Maizière, Minister of Interior, German Federal Ministry of Interior

Mr Nikos Paraskevopoulos, Minister of Justice, Hellenic Ministry of Justice, Transparency and Human Rights

Dr László Trócsányi, Minister of Justice, Hungarian Ministry of Justice

Mr Dara Murphy T.D., Minister for European Affairs and Data Protection, Department of the Taoiseach

Mr Andrea Orlando, Minister of Justice, Italian Ministry of Justice

Mr Dzintars Rasnačs, Minister of Justice, Latvian Ministry of Justice

Mr Juozas Bernatonis, Minister of Justice, Lithuanian Ministry of Justice

Mr Félix Braz, Minister of Justice, Luxembourg Ministry of Justice

Dr Owen Bonnici, Minister of Justice, Maltese Ministry of Justice, Culture and Local Government

Mr Zbigniew Ziobro, Minister of Justice, Polish Ministry of Justice

Ms Francisca Van Dunem, Minister of Justice, Portuguese Ministry of Justice

Ms Raluca Alexandra Prună, Minister of Justice, Romanian Ministry of Justice

JUDr. Tomáš Borec, Minister of Justice, Ministry of Justice of the Slovak Republic

Mr Goran Klemenčič, Minister of Justice, Slovenian Ministry of Justice

Mr Rafael Catalá, Minister of Justice, Spanish Ministry of Justice

Mr Morgan Johansson, Minister of Justice, Swedish Ministry of Justice and Migration

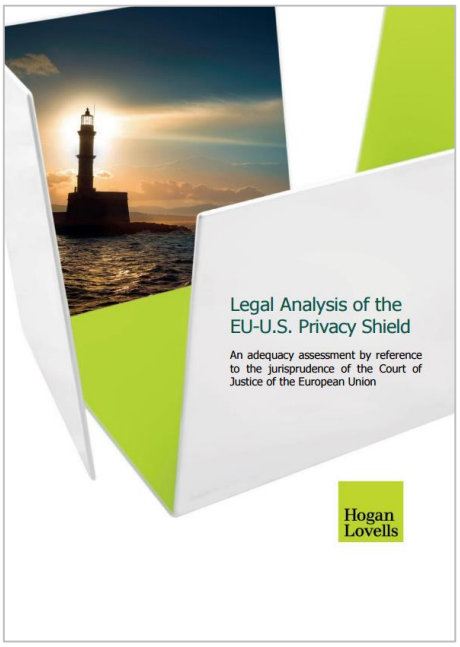
Baroness Neville-Rolfe, Under Secretary of State, United Kingdom Department for Culture, Media and Sport

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

Ms Tiina Astola, Director General, Directorate-General for Justice and Consumers, European Commission

ANNEX:

Extracted from the Legal Analysis of the EU-US Privacy Shield, *by Hogan Lovells.*



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.

Hogan Lovells

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.

DIGITALEUROPE
14, Rue de la Science 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

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.

DIGITALEUROPE
14, Rue de la Science 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

(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.

DIGITALEUROPE
14, Rue de la Science 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

- 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.

Hogan Lovells

(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.

DIGITALEUROPE
14, Rue de la Science 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

(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.