EUROPEAN
COMMISSION

Brussels, XXX
[…](2016) XXX draft

COMMISSION IMPLEMENTING DECISION

of XXX

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

(Text with EEA relevance)

COMMISSION IMPLEMENTING DECISION

of XXX

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

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and in particular Article 25(6) thereof,

After consulting the European Data Protection Supervisor,[2]

1. Introduction

(1) Directive 95/46/EC sets the rules for transfers of personal data from Member States to third countries to the extent that such transfers fall within its scope.

(2) Article 1 of Directive 95/46/EC and recitals 2 and 10 in its preamble seek to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms.[3]

(3) The importance of both the fundamental right to respect for private life, guaranteed by Article 7, and the fundamental right to the protection of personal data, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, has been emphasised in the case-law of the Court of Justice.[4]

(4) Pursuant to Article 25(1) of Directive 95/46/EC Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and the Member State laws implementing other provisions of the Directive are respected prior to the transfer. The

---

1 OJ L 281, 23.11.1995, p. 31.

2 See Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, published 30.05.2016.

3 Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* ("*Schrems*"), EU:C:2015:650, paragraph 39.

4 Case C-553/07, *Rijkeboer*, EU:C:2009:293, paragraph 47; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others*, EU:C:2014:238, paragraph 53; Case C-131/12, *Google Spain and Google*, EU:C:2014:317, paragraphs 53, 66 and 74.

Commission may find that a third country ensures such an adequate level of protection by reason of its domestic law or of the international commitments it has entered into in order to protect the rights of individuals. In that case, and without prejudice to compliance with the national provisions adopted pursuant to other provisions of the Directive, personal data may be transferred from the Member States without additional guarantees being necessary.

(5) Pursuant to Article 25(2) of Directive 95/46/EC, the level of data protection afforded by a third country should be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations, including the rules of law, both general and sectoral, in force in the third country in question.

(6) In Commission Decision 2000/520/EC[5], for the purposes of Article 25(2) of Directive 95/46/EC, the "Safe Harbour Privacy Principles", implemented in accordance with the guidance provided by the so-called "Frequently Asked Questions" issued by the U.S. Department of Commerce, were considered to ensure an adequate level of protection for personal data transferred from the Union to organisations established in the United States.

(7) In its Communications COM(2013) 846 final[6] and COM(2013) 847 final of 27 November 2013[7], the Commission considered that the fundamental basis of the Safe Harbour scheme had to be reviewed and strengthened in the context of a number of factors, including the exponential increase in data flows and their critical importance for the transatlantic economy, the rapid growth of the number of U.S. companies adhering to the Safe Harbour scheme and new information on the scale and scope of certain U.S. intelligence programs which raised questions as to the level of protection it could guarantee. In addition, the Commission identified a number of shortcomings and deficiencies in the Safe Harbour scheme.

(8) Based on evidence gathered by the Commission, including information stemming from the work of the EU-U.S. Privacy Contact Group[8] and the information on U.S. intelligence programs received in the ad hoc EU-U.S. Working Group[9], the Commission formulated 13 recommendations for a review of the Safe Harbour

---

5 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce (OJ L 215 of 28.8.2000, p. 7).

6 Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-U.S. Data Flows, COM(2013) 846 final of 27.11.2013.

7 Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies established in the EU, COM(2013) 847 final of 27.11.2013.

8 See e.g. Council of the European Union, Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, Note 9831/08, 28 May 2008, available on the internet at: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

9 Report on the Findings by the EU Co-chairs of the ad hoc EU-U.S. Working Group on Data Protection, 27.11.2013, available on the internet at: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

scheme. These recommendations focused on strengthening the substantive privacy principles, increasing the transparency of U.S. self-certified companies' privacy policies, better supervision, monitoring and enforcement by the U.S. authorities of compliance with those principles, the availability of affordable dispute resolution mechanisms, and the need to ensure that use of the national security exception provided in Commission Decision 2000/520/EC is limited to an extent that is strictly necessary and proportionate.

(9) In its judgment of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*[10], the Court of Justice of the European Union declared Commission Decision 2000/520/EC invalid. Without examining the content of the Safe Harbour Privacy Principles, the Court considered that the Commission had not stated in that decision that the United States in fact 'ensured' an adequate level of protection by reason of its domestic law or its international commitments.[11]

(10) In this regard, the Court of Justice explained that, while the term 'adequate level of protection' in Article 25(6) of Directive 95/46/EC does not mean a level of protection identical to that guaranteed in the EU legal order, it must be understood as requiring the third country to ensure a level of protection of fundamental rights and freedoms 'essentially equivalent' to that guaranteed within the Union by virtue of Directive 95/46/EC read in the light of the Charter of Fundamental Rights. Even though the means to which that third country has recourse, in this connection, may differ from the ones employed within the Union, those means must nevertheless prove, in practice, effective.[12]

(11) The Court of Justice criticised the lack of sufficient findings in Decision 2000/520/EC regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security, and the existence of effective legal protection against interference of that kind.[13]

(12) In 2014 the Commission had entered into talks with the U.S. authorities in order to discuss the strengthening of the Safe Harbour scheme in line with the 13 recommendations contained in Communication COM(2013) 847 final. After the judgment of the Court of Justice of the European Union in the *Schrems* case, these talks were intensified, with a view to a possible new adequacy decision which would meet the requirements of Article 25 of Directive 95/46/EC as interpreted by the Court of Justice. The documents which are annexed to this decision and will also be published in the U.S. Federal Register are the result of these discussions. The privacy principles (Annex II), together with the official representations and commitments by

---

[10] See footnote 3.

[11] *Schrems*, paragraph 97.

[12] *Schrems*, paragraphs 73-74.

[13] *Schrems*, paragraph 88-89.

various U.S. authorities contained in the documents in Annexes I, III to VII, constitute the "EU-U.S. Privacy Shield".

(13) The Commission has carefully analysed U.S. law and practice, including these official representations and commitments. Based on the findings developed in recitals (136)-(140), the Commission concludes that the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organisations in the United States.

2. The "EU-U.S. Privacy Shield"

(14) The EU-U.S. Privacy Shield is based on a system of self-certification by which U.S. organisations commit to a set of privacy principles – the EU-U.S. Privacy Shield Framework Principles, including the Supplemental Principles (hereinafter together: "the Principles") – issued by the U.S. Department of Commerce and contained in Annex II to this decision. It applies to both controllers and processors (agents), with the specificity that processors must be contractually bound to act only on instructions from the EU controller and assist the latter in responding to individuals exercising their rights under the Principles.[14]

(15) Without prejudice to compliance with the national provisions adopted pursuant to Directive 95/46/EC, the present decision has the effect that transfers from a controller or processor in the Union to organisations in the U.S. that have self-certified their adherence to the Principles with the Department of Commerce and have committed to comply with them are allowed. The Principles apply solely to the processing of personal data by the U.S. organisation in as far as processing by such organisations does not fall within the scope of Union legislation.[15] The Privacy Shield does not affect the application of Union legislation governing the processing of personal data in the Member States.[16]

---

[14] See Annex II, Sec. III.10.a. In line with the definition in Sec. I.8.c., the EU controller will determine the purpose and means of processing of the personal data. Moreover, the contract with the agent has to make clear whether onward transfers are allowed (see Sec. III.10.a.ii.2.).

[15] This applies also where human resources data transferred from the Union in the context of the employment relationship are concerned. While the Principles stress the "primary responsibility" of the EU employer (see Annex II, Sec. III.9.d.i.), they at the same time make clear that its conduct will be covered by the rules applicable in the Union and/or respective Member State, not the Principles. See Annex II, Sec. III.9.a.i., b.ii., c.i., d.i.

[16] This applies also to processing that takes place prior to the transfer to the United States through the use of equipment situated in the Union but used by an organisation established outside the Union (see Article 4(1)(c) of Directive 95/46/EC). As of 25 May 2018, the General Data Protection Regulation (GDPR) will apply to the processing of personal data (i) in the context of the activities of an establishment of a controller or processor in the Union (even where the processing takes place in the United States), or (ii) of data subjects who are in the Union by a controller or processor not established in the Union where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. See Article 3(1), (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 of 4.5.2016, p. 1.

(16) The protection afforded to personal data by the Privacy Shield applies to any EU data subject[17] whose personal data have been transferred from the Union to organisations in the U.S. that have self-certified their adherence to the Principles with the Department of Commerce.

(17) The Principles apply immediately upon certification. One exception relates to the Accountability for Onward Transfer Principle in a case where an organisation self-certifying to the Privacy Shield already has pre-existing commercial relationships with third parties. Given that it may take some time to bring those commercial relationships into conformity with the rules applicable under the Accountability for Onward Transfer Principle, the organisation will be obliged to do so as soon as possible, and in any event no later than nine months from self-certification (provided that this takes places in the first two months following the day when the Privacy Shield becomes effective). During this interim period, the organisation must apply the Notice and Choice Principle (thus allowing the EU data subject an opt-out) and, where personal data is transferred to a third party acting as an agent, must ensure that the latter provides at least the same level of protection as is required by the Principles.[18] This transitional period provides a reasonable and appropriate balance between the respect for the fundamental right to data protection and the legitimate needs of businesses to have sufficient time to adapt to the new framework where this also depends on their commercial relationships with third parties.

(18) The system will be administered and monitored by the Department of Commerce based on its commitments set out in the representations from the U.S. Secretary of Commerce (Annex I to this decision). With regard to the enforcement of the Principles, the Federal Trade Commission (FTC) and the Department of Transportation have made representations that are contained in Annex IV and Annex V to this decision.

2.1. Privacy Principles

(19) As part of their self-certification under the EU-U.S. Privacy Shield, organisations have to commit to comply with the Principles.[19]

---

[17] The present decision has EEA relevance. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Directive 95/46/EC, is covered by the EEA Agreement and has been incorporated into Annex XI thereof. The EEA Joint Committee has to decide on the incorporation of the present decision into the EEA Agreement. Once the present decision applies to Iceland, Liechtenstein and Norway, the EU-U.S. Privacy Shield will also cover these three countries and references in the Privacy Shield package to the EU and its Member States shall be read as including Iceland, Liechtenstein and Norway.

[18] See Annex II, Sec. III.6.e.

[19] Special rules providing additional safeguards apply for human resources data collected in the employment context as laid down in the supplemental principle on "Human Resources Data" of the Privacy Principles (See Annex II, Sec. III.9). For instance, employers should accommodate the privacy preferences of employees by restricting access to the personal data, anonymising certain data or assigning codes or pseudonyms. Most importantly, organisations are required to cooperate and comply with the advice of Union Data Protection Authorities when it comes to such data.

(20) Under the *Notice Principle*, organisations are obliged to provide information to data subjects on a number of key elements relating to the processing of their personal data (e.g. type of data collected, purpose of processing, right of access and choice, conditions for onward transfers and liability). Further safeguards apply, in particular the requirement for organisations to make public their privacy policies (reflecting the Principles) and to provide links to the Department of Commerce's website (with further details on self-certification, the rights of data subjects and available recourse mechanisms), the Privacy Shield List (referred to in recital (30)) and the website of an appropriate alternative dispute settlement provider.

(21) Under the *Data Integrity and Purpose Limitation Principle*, personal data must be limited to what is relevant for the purpose of the processing, reliable for its intended use, accurate, complete and current. An organisation may not process personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorised by the data subject. Organisations must ensure that personal data is reliable for its intended use, accurate, complete and current.

(22) Where a new (changed) purpose is materially different but still compatible with the original purpose, the *Choice Principle* gives data subjects the right to object (opt out). The *Choice Principle* does not supersede the express prohibition on incompatible processing.[20] Special rules generally allowing for the opt-out "at any time" from the use of personal data apply for direct marketing.[21] In the case of sensitive data, organisations must normally obtain the data subject's affirmative express consent (opt in).

(23) Still under the *Data Integrity and Purpose Limitation Principle*, personal information may be retained in a form identifying or rendering an individual identifiable (and thus in the form of personal data) only for as long as it serves the purpose(s) for which it was initially collected or subsequently authorised. This obligation does not prevent Privacy Shield organisations to continue processing personal information for longer periods, but only for the time and to the extent such processing reasonably serves one of the following specific purposes: archiving, journalism, literature and art, scientific and historical research and statistical analysis. Longer retention of personal data for one of these purposes will be subject to the safeguards provided by the Principles.

(24) Under the *Security Principle*, organisations creating, maintaining, using or disseminating personal data must take "reasonable and appropriate" security measures, taking into account the risks involved in the processing and the nature of the data. In the case of sub-processing, organisations must conclude a contract with the sub-

---

[20] This applies to all data transfers under the Privacy Shield, including where these concern data collected through the employment relationship. While a self-certified U.S. organisation may in principle use human resources data for different, non-employment-related purposes (e.g. certain marketing communications), it must respect the prohibition on incompatible processing and moreover may do so only in accordance with the *Notice* and *Choice Principles*. The prohibition on the U.S. organisation to take any punitive action against the employee for exercising such choice, including any restriction of employment opportunities, will ensure that, despite the relationship of subordination and inherent dependency, the employee will be free from pressure and thus can exercise a genuine free choice.

[21] See Annex II, Sec. III.12.

processor guaranteeing the same level of protection as provided by the Principles and take steps to ensure its proper implementation.

(25) Under the *Access Principle*,[22] data subjects have the right, without need for justification and only against a non-excessive fee, to obtain from an organisation confirmation of whether such organisation is processing personal data related to them and have the data communicated within reasonable time. This right may only be restricted in exceptional circumstances; any denial of, or limitation to the right of access has to be necessary and duly justified, with the organisation bearing the burden of demonstrating that these requirements are fulfilled. Data subjects must be able to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the Principles. In areas where companies most likely resort to the automated processing of personal data to take decisions affecting the individual (e.g. credit lending, mortgage offers, employment), U.S. law offers specific protections against adverse decisions.[23] These acts typically provide that individuals have the right to be informed of the specific reasons underlying the decision (e.g. the rejection of a credit), to dispute incomplete or inaccurate information (as well as reliance on unlawful factors), and to seek redress. These rules offer protections in the likely rather limited number of cases where automated decisions would be taken by the Privacy Shield organisation itself.[24] Nevertheless, given the increasing use of automated processing (including profiling) as a basis for taking decisions affecting individuals in the modern digital economy, this is an area that needs to be closely monitored. In order to facilitate this monitoring, it has been agreed with the U.S. authorities that a dialogue on automated decision-making, including an exchange on the similarities and differences in the EU and U.S. approach in this regard, will be part of the first annual review as well as subsequent reviews as appropriate.

(26) Under the *Recourse, Enforcement and Liability Principle*,[25] participating organisations must provide robust mechanisms to ensure compliance with the other Principles and recourse for EU data subjects whose personal data have been processed in a non-compliant manner, including effective remedies. Once an organisation has voluntarily decided to self-certify[26] under the EU-U.S. Privacy Shield, its effective compliance with the Principles is compulsory. To be allowed to continue to rely on the Privacy Shield to receive personal data from the Union, such organisation must annually re-certify its participation in the framework. Organisations must also take measures to

---

22 See also the supplemental principle on "Access" (Annex II, Sec. III.8).

23 See e.g. the Equal Credit Opportunity Act (ECOA, 15 U.S.C. 1691 et seq.), Fair Credit Reporting Act (FRCA, 15 USC § 1681 et seq.), or the Fair Housing Act (FHA, 42 U.S.C. 3601 et seq.).

24 In the context of a transfer of personal data that have been collected in the EU, the contractual relationship with the individual (customer) will in most cases be with – and therefore any decision based on automated processing will typically be taken by – the EU controller which has to abide by the EU data protection rules. This includes scenarios where the processing is carried out by a Privacy Shield organisation acting as an agent on behalf of the EU controller.

25 See also supplemental principle "Dispute Resolution and Enforcement" (Annex II, Sec. III.11).

26 See also supplemental principle "Self-Certification" (Annex II, Sec. III.6).

verify[27] that their published privacy policies conform to the Principles and are in fact complied with. This can be done either through a system of self-assessment, which must include internal procedures ensuring that employees receive training on the implementation of the organisation's privacy policies and that compliance is periodically reviewed in an objective manner, or outside compliance reviews, the methods of which may include auditing or random checks. In addition, the organisation must put in place an effective redress mechanism to deal with any complaints (see in this respect also recitals (43)) and be subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or another U.S. authorised statutory body that will effectively ensure compliance with the Principles.

(27) Special rules apply for so-called "onward transfers", i.e. transfers of personal data from an organisation to a third party controller or processor, irrespective of whether the latter is located in the United States or a third country outside the United States (and the Union). The purpose of these rules is to ensure that the protections guaranteed to the personal data of EU data subjects will not be undermined, and cannot be circumvented, by passing them on to third parties. This is particularly relevant in more complex processing chains which are typical for today's digital economy.

(28) Under the *Accountability for Onward Transfer Principle*,[28] any onward transfer can only take place (i) for limited and specified purposes, (ii) on the basis of a contract (or comparable arrangement within a corporate group[29]) and (iii) only if that contract provides the same level of protection as the one guaranteed by the Principles, which includes the requirement that the application of the Principles may only be limited to the extent necessary to meet national security, law enforcement and other public interest purposes.[30] This should be read in conjunction with the *Notice* and, in the case of an onward transfer to a third party controller[31], with the *Choice Principle*, according to which data subjects must be informed (among others) about the type/identity of any third party recipient, the purpose of the onward transfer as well as the choice offered and can object (opt out) or, in the case of sensitive data, have to give "affirmative express consent" (opt in) for onward transfers. In the light of the *Data Integrity and Purpose Limitation Principle*, the obligation to provide the same level of protection as guaranteed by the Principles presupposes that the third party may only process the personal information transmitted to it for purposes that are not incompatible with the

---

27 See also supplemental principle "Verification" (Annex II, Sec. III.7).

28 See also supplemental principle "Obligatory contracts for Onward Transfers" (Annex II, Sec. III.10).

29 See supplemental principle "Obligatory contracts for Onward Transfers" (Annex II, Sec. III.10.b). While this principle allows for transfers based also on non-contractual instruments (e.g., intra-group compliance and control programs), the text makes clear that these instruments must always "ensur[e] the continuity of protection of personal information under the Principles". Moreover, given that the self-certified U.S. organisation will remain responsible for compliance with the Principles it will have a strong incentive to use instruments that are indeed effective in practice.

30 See Annex II, Sec. I.5.

31 Individuals will have no opt-out right where the personal data is transferred to a third party that is acting as an agent to perform tasks on behalf of and under the instructions of the U.S. organisation. However, this requires a contract with the agent and the U.S. organisation will bear the responsibility to guarantee the protections provided under the Principles by exercising its powers of instruction.

purposes for which it was originally collected or subsequently authorised by the individual.

(29) The obligation to provide the same level of protection as required by the Principles applies to any and all third parties involved in the processing of the data so transferred irrespective of their location (in the U.S. or another third country) as well as when the original third party recipient itself transfers those data to another third party recipient, for example, for sub-processing purposes. In all cases, the contract with the third party recipient must provide that the latter will notify the Privacy Shield organisation if it makes a determination that it can no longer meet this obligation. When such a determination is made, the processing by the third party will cease or other reasonable and appropriate steps have to be taken to remedy the situation.[32] Where compliance problems arise in the (sub-) processing chain, the Privacy Shield organisation acting as the controller of the personal data will have to prove that it is not responsible for the event giving rise to the damage, or otherwise face liability, as specified in the *Recourse, Enforcement and Liability Principle*. Additional protections apply in the case of an onward transfer to a third party agent.[33]

2.2. Transparency, Administration and Oversight of the EU-U.S. Privacy Shield

(30) The EU-U.S. Privacy Shield provides for oversight and enforcement mechanisms in order to verify and ensure that U.S. self-certified companies comply with the Principles and that any failure to comply is addressed. These mechanisms are set out in the Principles (Annex II) and the commitments undertaken by the Department of Commerce (Annex I), the FTC (Annex IV) and the Department of Transportation (Annex V).

(31) To ensure the proper application of the EU-U.S. Privacy Shield, interested parties, such as data subjects, data exporters and the national Data Protection Authorities (DPAs), must be able to identify those organisations adhering to the Principles. To this end, the Department of Commerce has undertaken to maintain and make available to the public a list of organisations that have self-certified their adherence to the Principles and fall within the jurisdiction of at least one of the enforcement authorities referred to in Annexes I and II to this decision ("Privacy Shield List").[34] The Department of Commerce will update the list on the basis of an organisation's annual re-certification submissions and whenever an organisation withdraws or is removed

[32] The situation is different depending on whether the third party is a controller or a processor (agent). In the first scenario, the contract with the third party must provide that the latter ceases processing or takes other reasonable and appropriate steps to remedy the situation. In the second scenario, it is for the Privacy Shield organisation – as the one controlling the processing under whose instructions the agent operates – to take these measures.

[33] In such a case, the U.S. organisation must also take reasonable and appropriate steps (i) to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organisation's obligations under the Principles and, (ii) to stop and remediate unauthorised processing, upon notice.

[34] Information about the management of the Privacy Shield List can be found in Annex I and Annex II (Sec. I. 3, Sec. I.4, III.6.d, and Sec. III.11.g).

from the EU-U.S. Privacy Shield. It will also maintain and make available to the public an authoritative record of organisations that have been removed from the list, in each case identifying the reason for such removal. Finally, it will provide a link to the list of Privacy Shield-related FTC enforcement cases maintained on the FTC website.

(32) The Department of Commerce will make both the Privacy Shield List and the re-certification submissions publicly available through a dedicated website. Self-certified organisations must in turn provide the Department's web address for the Privacy Shield List. In addition, if available online, an organisation's privacy policy must include a hyperlink to the Privacy Shield website as well as a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints. The Department of Commerce will systematically verify, in the context of an organisation's certification and re-certification to the framework, that its privacy policies conform to the Principles.

(33) Organisations that have persistently failed to comply with the Principles will be removed from the Privacy Shield List and must return or delete the personal data received under the EU-U.S. Privacy Shield. In other cases of removal, such as voluntary withdrawal from participation or failure to recertify, the organisation may retain such data if it affirms to the Department of Commerce on an annual basis its commitment to continue to apply the Principles or provides adequate protection for the personal data by another authorised means (e.g. by using a contract that fully reflects the requirements of the relevant standard contractual clauses approved by the Commission). In this case, an organisation has to identify a contact point within the organisation for all Privacy Shield-related questions.

(34) The Department of Commerce will monitor organisations that are no longer members of the EU-U.S. Privacy Shield, either because they have voluntarily withdrawn or because their certification has lapsed, to verify whether they will return, delete or retain[35] the personal data received previously under the framework. If they retain these data, organisations are obliged to continue to apply the Principles to them. In cases where the Department of Commerce has removed organisations from the framework due to a persistent failure to comply with the Principles, it will ensure that those organisations return or delete the personal data they had received under the framework.

(35) When an organisation leaves the EU-U.S. Privacy Shield for any reason, it must remove all public statements implying that it continues to participate in the EU-U.S. Privacy Shield or is entitled to its benefits, in particular any references to the EU-U.S. Privacy Shield in its published privacy policy. The Department of Commerce will search for and address false claims of participation in the framework, including by former members.[36]Any misrepresentation to the general public by an organisation concerning its adherence to the Principles in the form of misleading statements or practices is subject to enforcement action by the FTC, Department of Transportation or

[35] See e.g. Annex II, Sec. I.3, Sec. III.6.f. and Sec. III.11.g.i.

[36] See Annex I, section on "Search for and Address False Claims of Participation".

other relevant U.S. enforcement authorities; misrepresentations to the Department of Commerce are enforceable under the False Statements Act (18 U.S.C. § 1001).[37]

(36) The Department of Commerce will *ex officio* monitor any false claims of Privacy Shield participation or the improper use of the Privacy Shield certification mark, and DPAs can refer organisations for review to a dedicated contact point at the Department. When an organisation has withdrawn from the EU-U.S. Privacy Shield, fails to re-certify or is removed from the Privacy Shield List, the Department of Commerce will on an on-going basis verify that it has deleted from its published privacy policy any references to the Privacy Shield that imply its continued participation and, if it continues to make false claims, refer the matter to the FTC, Department of Transportation or other competent authority for possible enforcement action. It will also send questionnaires to organisations whose self-certifications lapse or that have voluntarily withdrawn from the EU-U.S. Privacy Shield to verify whether the organisation will return, delete or continue to apply the Privacy Principles to the personal data that they received while participating in the EU-U.S. Privacy Shield and, if personal data are to be retained, verify who within the organisation will serve as an ongoing contact point for Privacy Shield-related questions.

(37) On an ongoing basis, the Department of Commerce will conduct *ex officio* compliance reviews[38] of self-certified organisations, including through sending detailed questionnaires. It will also systematically carry out reviews whenever it has received a specific (non-frivolous) complaint, when an organisation does not provide satisfactory responses to its enquiries, or when there is credible evidence suggesting that an organisation may not be complying with the Principles. Where appropriate, the Department of Commerce will also consult with DPAs about such compliance reviews.

2.3. Redress mechanisms, complaint handling and enforcement

(38) The EU-U.S. Privacy Shield, through the *Recourse, Enforcement and Liability Principle,* requires organisations to provide recourse for individuals who are affected by non-compliance and thus the possibility for EU data subjects to lodge complaints regarding non-compliance by U.S. self-certified companies and to have these complaints resolved, if necessary by a decision providing an effective remedy.

(39) As part of their self-certification, organisations must satisfy the requirements of the Recourse, Enforcement and Liability Principle by providing for effective and readily available independent recourse mechanisms by which each individual's complaints and disputes can be investigated and expeditiously resolved at no cost to the individual.

(40) Organisations may choose independent recourse mechanisms in either the Union or in the United States. This includes the possibility to voluntarily commit to cooperate with the EU DPAs. However, no such choice exists where organisations process human resources data as cooperation with the DPAs is then mandatory. Other alternatives

[37] See Annex II, Sec. III.6.h. and Sec. III.11.f.

[38] See Annex I.

include independent Alternative Dispute Resolution (ADR) or private-sector developed *privacy programs* that incorporate the Privacy Principles into their rules. The latter must include effective enforcement mechanisms in accordance with the requirements of the Recourse, Enforcement and Liability Principle. Organisations are obliged to remedy any problems of non-compliance. They must also specify that they are subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body.

(41) Consequently, the Privacy Shield framework provides data subjects with a number of possibilities to enforce their rights, lodge complaints regarding non-compliance by U.S. self-certified companies and to have their complaints resolved, if necessary by a decision providing an effective remedy. Individuals can bring a complaint directly to an organisation, to an independent dispute resolution body designated by the organisation, to national DPAs or to the FTC.

(42) In cases where their complaints have not been resolved by any of these recourse or enforcement mechanisms, individuals also have a right to invoke binding arbitration under the Privacy Shield Panel (Annex 1 of Annex II of this decision). Except for the arbitral panel, which requires certain remedies to be exhausted before it can be invoked, individuals are free to pursue any or all of the redress mechanism of their choice, and are not obliged to choose one mechanism over the other or to follow a specific sequence. However, there is a certain logical order that is advisable to follow, as set out below.

(43) First, EU data subjects may pursue cases of non-compliance with the Principles through direct contacts with the *U.S. self-certified company*. To facilitate resolution, the organisation must put in place an effective redress mechanism to deal with such complaints. An organisation's privacy policy must therefore clearly inform individuals about a contact point, either within or outside the organisation, that will handle complaints (including any relevant establishment in the Union that can respond to inquiries or complaints) and about the independent complaint handling mechanisms.

(44) Upon receipt of an individual's complaint, directly from the individual or through the Department of Commerce following referral by a DPA, the organisation must provide a response to the EU data subject within a period of 45 days. This response must include an assessment of the merits of the complaint and information as to how the organisation will rectify the problem. Likewise, organisations are required to respond promptly to inquiries and other requests for information from the Department of Commerce or from a DPA[39] (where the organisation has committed to cooperate with the DPA) relating to their adherence to the Principles. Organisations must retain their records on the implementation of their privacy policies and make them available upon request to an independent recourse mechanism or the FTC (or other U.S. authority with jurisdiction to investigate unfair and deceptive practices) in the context of an investigation or a complaint about non-compliance.

[39] This is the handling authority designated by the panel of DPAs provided for in the supplemental principle on "The Role of the Data Protection Authorities" (Annex II, Sec. III.5).

(45) Second, individuals can also bring a complaint directly to the *independent dispute resolution body* (either in the United States or in the Union) designated by an organisation to investigate and resolve individual complaints (unless they are obviously unfounded or frivolous) and to provide appropriate recourse free of charge to the individual. Sanctions and remedies imposed by such a body must be sufficiently rigorous to ensure compliance by organisations with the Principles and should provide for a reversal or correction by the organisation of the effects of non-compliance and, depending on the circumstances, the termination of the further processing of the personal data at stake and/or their deletion, as well as publicity for findings of non-compliance. Independent dispute resolution bodies designated by an organisation will be required to include on their public websites relevant information regarding the EU-U.S. Privacy Shield and the services they provide under it. Each year, they must publish an annual report providing aggregate statistics regarding these services.[40]

(46) As part of its compliance review procedures, the Department of Commerce will verify that self-certified U.S. companies have actually registered with the independent recourse mechanisms they claim they are registered with. Both the organisations and the responsible independent recourse mechanisms are required to respond promptly to inquiries and requests by the Department of Commerce for information relating to the Privacy Shield.

(47) In cases where the organisation fails to comply with the ruling of a dispute resolution or self-regulatory body, the latter must notify such non-compliance to the Department of Commerce and the FTC (or other U.S. authority with jurisdiction to investigate unfair and deceptive practices), or a competent court.[41] If an organisation refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution or government body or where such a body determines that an organisation frequently fails to comply with the Principles, this will be considered as a persistent failure to comply with the result that the Department of Commerce, after first providing 30 days' notice and an opportunity to respond to the organization that has failed to comply, will strike the organisation off the list.[42] If, after removal from the list, the organisation continues to make the claim of Privacy Shield certification, the Department will refer it to the FTC or other enforcement agency.[43]

(48) Third, individuals may also bring their complaints to a national *Data Protection Authority*. Organisations are obliged to cooperate in the investigation and the resolution of a complaint by a DPA either when it concerns the processing of human resources data collected in the context of an employment relationship or when the respective organisation has voluntarily submitted to the oversight by DPAs. Notably, organisations have to respond to inquiries, comply with the advice given by the DPA,

---

[40] The annual report must include: (1) the total number of Privacy Shield-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed**.**

[41] See Annex II, Sec. III.11.e.

[42] See Annex II, Sec. III.11.g, in particular points (ii) and (iii).

[43] See Annex I, section on "Search for and Address False Claims of Participation".

including for remedial or compensatory measures, and provide the DPA with written confirmation that such action has been taken.

(49) The advice of the DPAs will be delivered through an informal panel of DPAs established at Union level,[44] which will help to ensure a harmonised and coherent approach to a particular complaint. Advice will be issued after both sides in the dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will deliver advice as quickly as the requirement for due process allows, and as a general rule within 60 days after receiving a complaint. If an organisation fails to comply within 25 days of delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to submit the matter to the FTC (or other competent U.S. enforcement authority), or to conclude that the commitment to cooperate has been seriously breached. In the first alternative, this may lead to enforcement action based on Section 5 of the FTC Act (or similar statute). In the second alternative, the panel will inform the Department of Commerce which will consider the organisation's refusal to comply with the advice of the DPA panel as a persistent failure to comply that will lead to the organisation's removal from the Privacy Shield List.

(50) If the DPA to which the complaint has been addressed has taken no or insufficient action to address a complaint, the individual complainant has the possibility to challenge such (in-) action in the national courts of the respective Member State.

(51) Individuals may also bring complaints to DPAs even when the DPA panel has not been designated as an organisation's dispute resolution body. In these cases, the DPA may refer such complaints either to the Department of Commerce or the FTC. In order to facilitate and increase cooperation on matters relating to individual complaints and non-compliance by Privacy Shield organisations, the Department of Commerce will establish a dedicated contact point to act as a liaison and to assist with DPA inquiries regarding an organisation's compliance with the Principles.[45] Likewise, the FTC has committed to establish a dedicated point of contact[46] and provide the DPAs with investigatory assistance pursuant to the U.S. SAFE WEB Act.47

(52) Fourth, the *Department of Commerce* has committed to receive, review and undertake best efforts to resolve complaints about an organisation's non-compliance with the Principles. To this end, the Department of Commerce provides special procedures for DPAs to refer complaints to a dedicated contact point, track them and follow up with companies to facilitate resolution. In order to expedite the processing of individual complaints, the contact point will liaise directly with the respective DPA on compliance issues and in particular update it on the status of complaints within a period of not more than 90 days following referral. This allows data subjects to bring

---

44 The rules of procedure of the informal DPA panel should be established by the DPAs based on their competence to organise their work and cooperate among each other.

45 See Annex I, sections on "Increase Cooperation with DPAs" and "Facilitate Resolution of Complaints about Non-Compliance" and Annex II, Sec. II.7.e.

46 See Annex IV, p.6.

47 *ibid*.

complaints of non-compliance by U.S. self-certified companies directly to their national DPA and have them channelled to the Department of Commerce as the U.S. authority administering the EU-U.S. Privacy Shield. The Department of Commerce has also committed to provide, in the annual review of the functioning of the EU-U.S. Privacy Shield, a report that analyses in aggregate form the complaints it receives each year.[48]

(53) Where, on the basis of its *ex officio* verifications, complaints or any other information, the Department of Commerce concludes that an organisation has persistently failed to comply with the Privacy Principles it will remove such an organisation from the Privacy Shield list. Refusal to comply with a final determination by any privacy self-regulatory, independent dispute resolution or government body, including a DPA, will be regarded as a persistent failure to comply.

(54) Fifth, a Privacy Shield organisation must be subject to the investigatory and enforcement powers of the U.S. authorities, in particular the *Federal Trade Commission*[49] that will effectively ensure compliance with the Principles. The FTC will give priority consideration to referrals of non-compliance with the Privacy Principles received from independent dispute resolution or self-regulatory bodies, the Department of Commerce and DPAs (acting on their own initiative or upon complaints) to determine whether Section 5 of the FTC Act has been violated.[50] The FTC has committed to create a standardised referral process, to designate a point of contact at the agency for DPA referrals, and to exchange information on referrals. In addition, it will accept complaints directly from individuals and will undertake Privacy Shield investigations on its own initiative, in particular as part of its wider investigations of privacy issues.

(55) The FTC can enforce compliance through administrative orders ("consent orders"), and it will systematically monitor compliance with such orders. Where organisations fail to comply, the FTC may refer the case to the competent court in order to seek civil penalties and other remedies, including for any injury caused by the unlawful conduct. Alternatively, the FTC may directly seek a preliminary or permanent injunction or other remedies from a federal court. Each consent order issued to a Privacy Shield organisation will have self-reporting provisions[51], and organisations will be required to make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC. Finally, the FTC will maintain an online list of companies subject to FTC or court orders in Privacy Shield cases.

---

48 See Annex I, section on "Facilitate Resolution of Complaints about Non-Compliance".

49 A Privacy Shield organisation has to publicly declare its commitment to comply with the Principles, publicly disclose its privacy policies in line with these Principles and fully implement them. Failure to comply is enforceable under Section 5 of the FTC Act prohibiting unfair and deceptive acts in or affecting commerce.

50 According to information from the FTC, it has no power to conduct on-site inspections in the area of privacy protection. However, it has the power to compel organisations to produce documents and provide witness statements (see Section 20 of the FTC Act), and may use the court system to enforce such orders in case of non-compliance.

51 FTC or court orders may require companies to implement privacy programs and to regularly make compliance reports or independent third-party assessments of those programs available to the FTC.

(56) Sixth, as a recourse mechanism of 'last resort' in case none of the other available redress avenues has satisfactorily resolved an individual's complaint, the EU data subject may invoke binding arbitration by the *"Privacy Shield Panel"*. Organisations must inform individuals about their possibility, under certain conditions, to invoke binding arbitration and they are obliged to respond once an individual has invoked this option by delivering notice to the concerned organisation.[52]

(57) This arbitral panel will consist of a pool of at least 20 arbitrators designated by the Department of Commerce and the Commission based on their independence, integrity, as well as experience in U.S. privacy and Union data protection law. For each individual dispute, the parties will select from this pool a panel of one or three[53] arbitrators. The proceedings will be governed by standard arbitration rules to be agreed between the Department of Commerce and the Commission. These rules will supplement the already concluded framework which contains several features which enhance the accessibility of this mechanism for EU data subjects: (i) in preparing a claim before the panel, the data subject may be assisted by his or her national DPA; (ii) while the arbitration will take place in the United States, EU data subjects may choose to participate through video or telephone conference, to be provided at no cost to the individual; (iii) while the language used in the arbitration will as a rule be English, interpretation at the arbitral hearing and translation will normally[54] be provided upon a reasoned request and at no cost to the data subject; (iv) finally, while each party has to bear its own attorney's fees, if represented by an attorney before the panel, the Department of Commerce will establish a fund supplied with annual contributions by the Privacy Shield organisations, which shall cover the eligible costs of the arbitration procedure, up to maximum amounts, to be determined by the U.S. authorities in consultation with the Commission.

(58) The Privacy Shield Panel will have the authority to impose "individual-specific, non-monetary equitable relief"[55] necessary to remedy non-compliance with the Principles. While the panel will take into account other remedies already obtained by other Privacy Shield mechanisms when making its determination, individuals may still resort to arbitration if they consider these other remedies to be insufficient. This will allow EU data subjects to invoke arbitration in all cases where the action or inaction of the competent U.S. authorities (for instance the FTC) has not satisfactorily resolved their complaints. Arbitration may not be invoked if a DPA has the legal authority to resolve the claim at issue with respect to the U.S. self-certified company, namely in those cases where the organisation is either obliged to cooperate and comply with the advice of the DPAs as regards the processing of human resources data collected in the employment context, or has voluntarily committed to do so. Individuals can enforce

---

52 See Annex II, Sec. II.1.xi and III.7.c.

53 The number of arbitrators on the panel will have to be agreed between the parties.

54 However, the panel may find that, under the circumstances of the specific arbitration, coverage would lead to unjustified or disproportionate costs.

55 Individuals may not claim damages in arbitration, but in turn invoking arbitration will not foreclose the option to seek damages in the ordinary U.S. courts.

the arbitration decision in the U.S. courts under the Federal Arbitration Act, thereby ensuring a legal remedy in case a company fails to comply.

(59) Seventh, where an organisation does not comply with its commitment to respect the Principles and published privacy policy, additional avenues for judicial redress may be available under the law of the U.S. States which provide for legal remedies under tort law and in cases of fraudulent misrepresentation, unfair or deceptive acts or practices, or breach of contract.

(60) Ultimately, where a DPA, upon receiving a claim by an EU data subject, considers that the individual's personal data transferred to an organisation in the United States are not afforded an adequate level of protection, it can also exercise its powers vis-à-vis the data exporter and, if necessary, suspend the data transfer.

(61) In the light of the information in this section, the Commission considers that the Principles issued by the U.S. Department of Commerce as such 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.

(62) In addition, the effective application of the Principles is guaranteed by the transparency obligations, and the administration and compliance review of the Privacy Shield by the Department of Commerce.

(63) Moreover, the Commission considers that, taken as a whole, the oversight, recourse and enforcement mechanisms provided for by the Privacy Shield enable infringements of the 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.

3. Access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities

(64) As follows from Annex II, Sec. I.5, adherence to the Principles is limited to the extent necessary to meet national security, public interest or law enforcement requirements.

(65) The Commission has assessed the limitations and safeguards available in U.S. law as regards access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities for national security, law enforcement and other public interest purposes. In addition, the U.S. government, through its Office of the Director of National Intelligence (ODNI)[56], has provided the Commission with detailed representations and commitments that are contained in Annex VI to this decision. By letter signed by the Secretary of State and attached as Annex III to this decision the U.S. government has also committed to create a new oversight mechanism for national

[56] The Director of National Intelligence (DNI) serves as the head of the Intelligence Community and acts as the principal advisor to the President and the National Security Council. See the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 of 17.12.2004. Among others, the ODNI shall determine requirements for, and manage and direct the tasking, collection, analysis, production and dissemination of national intelligence by the Intelligence Community, including by developing guidelines for how information or intelligence is accessed, used and shared. See Sec. 1.3 (a), (b) of E.O. 12333.

security interference, the Privacy Shield Ombudsperson, who is independent from the Intelligence Community. Finally, a representation from the U.S. Department of Justice, contained in Annex VII to this decision, describes the limitations and safeguards applicable to access and use of data by public authorities for law enforcement and other public interest purposes. In order to enhance transparency and to reflect the legal nature of these commitments, each of the documents listed and annexed to this decision will be published in the U.S. Federal Register.

(66) The findings of the Commission on the limitations on access and use of personal data transferred from the European Union to the United States by U.S. public authorities and the existence of effective legal protection are further elaborated below.

3.1. Access and use by U.S. public authorities for national security purposes

(67) The Commission's analysis shows that U.S. law contains a number of limitations on the access and use of personal data transferred under the EU-U.S. Privacy Shield for national security purposes as well as oversight and redress mechanisms that provide sufficient safeguards for those data to be effectively protected against unlawful interference and the risk of abuse.[57] Since 2013, when the Commission issued its two Communications (see recital (7)), this legal framework has been significantly strengthened, as described below.

3.1.1. Limitations

(68) Under the U.S. Constitution, ensuring national security falls within the President's authority as Commander in Chief, as Chief Executive and, as regards foreign intelligence, to conduct U.S. foreign affairs.[58] While Congress has the power to impose limitations, and has done so in various respects, within these boundaries the President may direct the activities of the U.S. Intelligence Community, in particular through Executive Orders or Presidential Directives. This of course also applies in those areas where no Congressional guidance exists. At present, the two central legal instruments in this regard are Executive Order 12333 ("E.O. 12333")[59] and Presidential Policy Directive 28.

(69) Presidential Policy Directive 28 ("PPD-28"), issued on 17 January 2014, imposes a number of limitations for "signals intelligence" operations.[60] This presidential

---

57 See *Schrems*, paragraph 91.

58 U.S. Const., Article II. See also the introduction to PPD-28.

59 E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No. 235 (8.12.1981). To the extent that the Executive Order is publicly accessible, it defines the goals, directions, duties and responsibilities of U.S. intelligence efforts (including the role of the various Intelligence Community elements) and sets out the general parameters for the conduct of intelligence activities (in particular the need to promulgate specific procedural rules). According to Sec. 3.2 of E.O. 12333, the President, supported by the National Security Council, and the DNI shall issue such appropriate directives, procedures and guidance as are necessary to implement the order.

60 According to E.O. 12333, the Director of the National Security Agency (NSA) is the Functional Manager for signals intelligence and shall operate a unified organization for signals intelligence activities.

directive has binding force for U.S. intelligence authorities[61] and remains effective upon change in the U.S. Administration.[62] PPD-28 is of particular importance for non-US persons, including EU data subjects. Among others, it stipulates that:

(a) the collection of signals intelligence must be based on statute or Presidential authorisation, and must be undertaken in accordance with the U.S. Constitution (in particular the Fourth Amendment) and U.S. law;

(b) all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside;

(c) all persons have legitimate privacy interests in the handling of their personal information;

(d) privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities;

(e) U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of their nationality or where they might reside.

(70) PPD-28 directs that signals intelligence may be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purpose (e.g. to afford a competitive advantage to U.S. companies). In this regard, the ODNI explains that Intelligence Community elements "should require that, wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (*e.g.* specific facilities, selection terms and identifiers)."[63] Furthermore, the representations provide assurance that decisions about intelligence collection are not left to the discretion of individual intelligence agents, but are subject to the policies and procedures that the various U.S. Intelligence Community elements (agencies) are required to put in place to implement PPD-28.[64] Accordingly, the research and determination of appropriate selectors takes place within the overall "National Intelligence Priorities Framework" (NIPF) which ensures that intelligence priorities are set by high-level policymakers and regularly reviewed to remain responsive to actual national security threats and taking into account possible risks, including privacy risks.[65] On this basis, agency personnel researches and identifies specific selection terms expected to collect foreign intelligence responsive to the

---

[61] For the definition of the term "Intelligence Community", see Sec. 3.5 (h) of E.O. 12333 with n. 1 of PPD-28.

[62] See Memorandum by the Office of Legal Counsel, Department of Justice (DOJ), to President Clinton, 29.01.2000. According to this legal opinion, presidential directives have the "same substantive legal effect as an Executive Order".

[63] ODNI Representations (Annex VI), p. 3.

[64] See Sec. 4(b),(c) of PPD-28. According to public information, the 2015 review confirmed the existing six purposes. See ODNI, Signals Intelligence Reform, 2016 Progress Report.

[65] ODNI Representations (Annex VI), p. 6 (with reference to Intelligence Community Directive 204). See also Sec. 3 of PPD-28.

priorities.[66] Selection terms, or "selectors", must be regularly reviewed to see if they still provide valuable intelligence in line with the priorities.[67]

(71) Furthermore, the requirements stipulated in PPD-28 that intelligence collection shall always[68] be "as tailored as feasible", and that the Intelligence Community shall prioritise the availability of other information and appropriate and feasible alternatives,[69] reflect a general rule of prioritisation of targeted over bulk collection. According to the assurance provided by the ODNI, they ensure in particular that bulk collection is neither "mass" nor "indiscriminate", and that the exception does not swallow the rule.[70]

(72) While PPD-28 explains that Intelligence Community elements must sometimes collect bulk signals intelligence in certain circumstances, for instance in order to identify and assess new or emerging threats, it directs these elements to prioritise alternatives that would allow the conduct of targeted signals intelligence.[71] It follows that bulk collection will only occur where targeted collection via the use of discriminants – i.e. an identifier associated with a specific target (such as the target's email address or phone number) – is not possible "due to technical or operational considerations".[72] This applies both to the manner in which signals intelligence is collected and to what is actually collected.[73]

(73) According to the representations from the ODNI, even where the Intelligence Community cannot use specific identifiers to target collection, it will seek to narrow the collection "as much as possible". In order to ensure this, it "applies filters and other technical tools to focus the collection on those facilities that are likely to contain

---

66 ODNI Representations (Annex VI), p. 6. See, for instance, NSA Civil Liberties and Privacy Office (NSA CLPO), NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014. See also ODNI Status Report 2014. For access requests under Sec. 702 FISA, queries are governed by the FISC-approved minimization procedures. See NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014.

67 See Signal Intelligence Reform, 2015 Anniversary Report. See also ODNI Representations (Annex VI), pp. 6, 8-9, 11.

68 See ODNI Representations (Annex VI), p. 3.

69 It should also be noted that, according to Sec. 2.4 of E.O. 12333, elements of the IC "shall use the least intrusive collection techniques feasible within the United States". As regards the limitations for substituting all bulk collection with targeted collections, see the results of an assessment by the National Research Council as reported by the European Union Agency for Fundamental Rights, Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU (2015), p.18.

70 ODNI Representations (Annex VI), p. 4.

71 See also Sec. 5(d) of PPD-28 which directs the Director of National Intelligence, in coordination with the heads of relevant Intelligence Community elements and the Office of Science and Technology Policy, to provide the President with a "report assessing the feasibility of creating software that would allow the Intelligence Community more easily to conduct targeted information acquisition rather than bulk collection." According to public information, the result of this report was that "there is no software-based alternative which will provide a complete substitute for bulk collection in the detection of some national security threats." See Signals Intelligence Reform, 2015 Anniversary Report.

72 See ODNI Representations (Annex VI), p. 3.

73 ODNI Representations (Annex VI), p. 3.

communications of foreign intelligence value" (and thus will be responsive to requirements articulated by U.S. policy-makers pursuant to the process described above in (70)). As a consequence, bulk collection will be targeted in at least two ways: First, it will always relate to specific foreign intelligence objectives (e.g. to acquire signals intelligence about the activities of a terrorist group operating in a particular region) and focus collection on communications that have such a nexus. According to the assurance provided by the ODNI, this is reflected in the fact that the "United States' signals intelligence activities touch only a fraction of the communications traversing the internet."[74] Second, the ODNI representations explain that the filters and other technical tools used will be designed to focus the collection "as precisely as possible" in order to ensure that the amount of "non-pertinent information" collected will be minimised.

(74) Finally, even where the United States considers it necessary to collect signals intelligence in bulk, under the conditions set out in recitals (70)-(73), PPD-28 limits the use of such information to a specific list of six national security purposes with a view to protect the privacy and civil liberties of all persons, whatever their nationality and place of residence.[75] These permissible purposes comprise measures to detect and counter threats stemming from espionage, terrorism, weapons of mass destruction, to the Armed Forces or military personnel, as well as transnational criminal threats related to the other five purposes, and will be reviewed at least on an annual basis. According to the representations by the U.S. government, Intelligence Community elements have reinforced their analytic practices and standards for querying unevaluated signals intelligence to conform with these requirements; the use of targeted queries "ensures that only those items believed to be of potential intelligence value are ever presented to analysts to examine."[76]

(75) These limitations are particularly relevant to personal data transferred under the EU-U.S. Privacy Shield, in particular in case access to personal data were to take place outside the United States, including during their transit on the transatlantic cables from the Union to the United States. As confirmed by the U.S. authorities in the representations of the ODNI, the limitations and safeguards set out therein – including those of PPD-28 – apply to such access.[77]

(76) Although not phrased in those legal terms, these principles capture the essence of the principles of necessity and proportionality. Targeted collection is clearly prioritised, while bulk collection is limited to (exceptional) situations where targeted collection is not possible for technical or operational reasons. Even where *bulk collection* cannot be

---

[74] This specifically addresses the concern expressed by the national data protection authorities in their opinion on the draft adequacy decision. See Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (adopted 13.4.2016), p. 38 with n. 47.

[75] See Sec. 2 of PPD-28.

[76] ODNI Representations (Annex VI), p. 4. See also Intelligence Community Directive 203.

[77] ODNI Representations (Annex VI), p. 2. Likewise, the limitations stipulated in E.O. 12333 (e.g. the need for collected information to respond to intelligence priorities set by the President) apply.

avoided, further "use" of such data through access is *strictly limited* to specific, legitimate national security purposes.[78]

(77) As a directive issued by the President as the Chief Executive, these requirements bind the entire Intelligence Community and have been further implemented through agency rules and procedures that transpose the general principles into specific directions for day-to-day operations. Moreover, while Congress is itself not bound by PPD-28, it has also taken steps to ensure that collection and access of personal data in the United States are targeted rather than carried out "on a generalised basis".

(78) It follows from the available information, including the representations received from the U.S. government, that once the data has been transferred to organisations located in the United States and self-certified under the EU-U.S. Privacy Shield, U.S. intelligence agencies may only[79] seek personal data where their request complies with the Foreign Intelligence Surveillance Act (FISA) or is made by the Federal Bureau of Investigation (FBI) based on a so-called National Security Letter (NSL)[80]. Several legal bases exist under FISA that may be used to collect (and subsequently process) the personal data of EU data subjects transferred under the EU-U.S. Privacy Shield. Aside from Section 104 FISA[81] covering traditional individualised electronic surveillance and Section 402 FISA[82] on the installation of pen registers or trap and

---

78 See *Schrems*, paragraph 93.

79 In addition, the collection of data by the FBI may also be based on law enforcement authorizations (see Section 3.2 of this decision).

80 For further explanations on the use of NSL see ODNI Representations (Annex VI), pp. 13-14 with n. 38. As indicated therein, the FBI may resort to NSLs only to request non-content information relevant to an authorized national security investigation to protect against international terrorism or clandestine intelligence activities. As regards data transfers under the EU-U.S. Privacy Shield, the most relevant legal authorization appears to be the Electronic Communications Privacy Act (18 U.S.C. § 2709), which requires that any request for subscriber information or transactional records uses a "term that specifically identifies a person, entity, telephone number, or account".

81 50 U.S.C. § 1804. While this legal authority requires a "statement of the facts and circumstances relied upon by the applicant to justify his belief that (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power", the latter may include non-U.S. persons that engage in international terrorism or the international proliferation of weapons of mass destruction (including preparatory acts) (50 U.S.C. § 1801 (b)(1)). Still, there is only a theoretical link to personal data transferred under the EU-U.S. Privacy Shield, given that the statement of facts also has to justify the belief that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power". In any event, the use of this authority requires application to the FISC which will assess, among others, whether on the basis of the submitted facts there is probable cause that this is indeed the case.

82 50 U.S.C. § 1842 with § 1841(2) and Sec. 3127 of Title 18. This authority does not concern the contents of communications, but rather aims at information about the customer or subscriber using a service (such as name, address, subscriber number, length/type of service received, source/mechanism of payment). It requires an application for an order by the FISC (or a U.S. Magistrate Judge) and the use of a specific selection term in the sense of § 1841(4), i.e. a term that specifically identifies a person, account, etc. and is used to limit, to the greatest extent reasonably possible, the scope of the information sought.

trace devices, the two central instruments are Section 501 FISA (ex-Section 215 U.S. PATRIOT ACT) and Section 702 FISA.[83]

(79) In this respect, the USA FREEDOM Act, which was enacted on 2 June 2015, prohibits the collection in bulk of records based on Section 402 FISA (pen register and trap and trace authority), Section 501 FISA (formerly: Section 215 of the U.S. PATRIOT ACT)[84] and through the use of NSL, and instead requires the use of specific "selection terms".[85]

(80) While the FISA contains further legal authorisations to carry out national intelligence activities, including signals intelligence, the Commission's assessment has shown that, insofar as personal data to be transferred under the EU-U.S. Privacy Shield are concerned, these authorities equally restrict interference by public authorities to targeted collection and access.

(81) This is clear for traditional individualised electronic surveillance under Section 104 FISA.[86] As for Section 702 FISA, which provides the basis for two important intelligence programs run by the U.S. intelligence agencies (PRISM, UPSTREAM), searches are carried out in a targeted manner through the use of individual selectors that identify specific communications facilities, like the target's email address or telephone number, but not key words or even the names of targeted individuals.[87] Therefore, as noted by the Privacy and Civil Liberties Oversight Board (PCLOB), Section 702 surveillance "consists entirely of targeting specific [non-U.S.] persons about whom an individualised determination has been made".[88] Due to a "sunset"

---

83 While Sec. 501 FISA (ex-Sec. 215 U.S. PATRIOT ACT) authorizes the FBI to request a court order aiming at the production of "tangible things" (in particular telephone metadata, but also business records) for foreign intelligence purposes, Sec. 702 FISA allows US Intelligence Community elements to seek access to information, including the content of internet communications, from within the United States, but targeting certain non-U.S. persons outside the United States.

84 Based on this provision, the FBI may request "tangible things" (e.g. records, papers, documents) based on a showing to the Foreign Intelligence Surveillance Court (FISC) that there are reasonable grounds to believe that they are relevant to a specific FBI investigation. In carrying out its search, the FBI must use FISC-approved selection terms for which there is a "reasonable, articulable suspicion" that such term is associated with one or more foreign powers or their agents engaged in international terrorism or activities in preparation therefore. See PCLOB, Sec. 215 Report, p. 59; NSA CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.01.2016, pp. 4-6.

85 ODNI Representations (Annex VI), p. 13 (n. 38).

86 See footnote 81.

87 PCLOB, Sec. 702 Report, pp. 32-33 with further references. According to its privacy office, the NSA must verify that there is a connection between the target and the selector, must document the foreign intelligence information expected to be acquired, this information must be reviewed and approved by two senior NSA analysts, and the overall process will be tracked for subsequent compliance reviews by the ODNI and Department of Justice. See NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.04.2014.

88 PLCOB, Sec. 702 Report, p. 111. See also ODNI Representations (Annex VI), p. 9 ("Collection under Section 702 of the [FISA] is not 'mass and indiscriminate' but is narrowly focused on the collection of foreign intelligence from individually identified legitimate targets") and p. 13, n. 36 (with reference to a 2014 FISC Opinion); NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.04.2014. Even in the case of UPSTREAM, the NSA may only request the interception of electronic communications to, from, or about tasked selectors.

clause, Section 702 FISA will have to be reviewed in 2017, at which time the Commission will have to reassess the safeguards available to EU data subjects.

(82) Moreover, in its representations the U.S. government has given the European Commission explicit assurance that the U.S. Intelligence Community "does not engage in indiscriminate surveillance of anyone, including ordinary European citizens"[89]. As regards personal data collected within the United States, this statement is supported by empirical evidence which shows that *access requests* through NSL and under FISA, both individually and together, only concern a relatively small number of targets when compared to the overall flow of data on the internet.[90] Moreover, the U.S. government has assured the Commission that United States' signals intelligence activities touch only a fraction of the communications traversing the Internet."[91] This statement also covers possible access to the transatlantic cables (which the U.S. government neither confirms nor denies is taking place).

(83) As regards *access* to collected data and *data security*, PPD-28 requires that access "shall be limited to authorized personnel with a need to know the information to perform their mission" and that personal information "shall be processed and stored under conditions that provide adequate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information". Intelligence personnel receive appropriate and adequate training in the principles set forth in PPD-28.[92]

(84) Finally, as regards the *storage* and further *dissemination* of personal data from EU data subjects collected by U.S. intelligence authorities, PPD-28 states that all persons (including non-U.S. persons) should be treated with dignity and respect, that all persons have legitimate privacy interests in the handling of their personal data and that

---

89 ODNI Representations (Annex VI), p. 18. See also p. 6, according to which the applicable procedures "demonstrate a clear commitment to prevent arbitrary and indiscriminate collection of signals intelligence information, and to implement – from the highest levels of our Government – the principle of reasonableness."

90 See Statistical Transparency Report Regarding Use of National Security Authorities, 22.04.2015. For the overall flow of data on the internet, see for example Fundamental Rights Agency, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (2015), at pp. 15-16. As regards the UPSTREAM program, according to a declassified FISC opinion of 2011, over 90% of the electronic communications acquired under Sec. 702 FISA came from the PRISM program, whereas less than 10% came from UPSTREAM. See FISC, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 3.10.2011), n. 21 (available at: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

91 ODNI Representations (Annex VI), p. 4.

92 See Sec. 4(a)(ii) of PPD-28. See also ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, July 2014, p. 5, according to which "Intelligence Community element policies should reinforce existing analytic practices and standards whereby analysts must seek to structure queries or other search terms and techniques to identify intelligence information relevant to a valid intelligence or law enforcement task; focus queries about persons on the categories of intelligence information responsive to an intelligence or law enforcement requirement; and minimize the review of personal information not pertinent to intelligence or law enforcement requirements." See e.g. CIA, Signals Intelligence Activities, p. 5; FBI, Presidential Policy Directive 28 Policies and Procedures, p. 3. According to the 2016 Progress Report on the Signals Intelligence Reform, IC elements (including the FBI, CIA and NSA) have taken steps to sensitise their personnel to the requirements of PPD-28 by creating new or modifying existing training policies.

Intelligence Community elements therefore have to establish policies providing appropriate safeguards for such data "reasonably designed to minimize the[ir] dissemination and retention".[93]

(85) The U.S. government has explained that this reasonableness requirement signifies that Intelligence Community elements will not have to adopt "any measure theoretically possible", but will need to "balance their efforts to protect legitimate privacy and civil liberties interests with the practical necessities of signals intelligence activities."[94] In this respect, non-U.S. persons will be treated in the same way as U.S. persons, based on procedures approved by the Attorney-General.[95]

(86) According to these rules, retention is generally limited to a maximum of five years, unless there is a specific determination in law or an express determination by the Director of National Intelligence after careful evaluation of privacy concerns – taking into account the views of the ODNI Civil Liberties Protection Officer as well as agency privacy and civil liberties officials – that continued retention is in the interest of national security.[96] Dissemination is limited to cases where the information is relevant to the underlying purpose of the collection and thus responsive to an authorised foreign intelligence or law enforcement requirement.[97]

(87) According to the assurances given by the U.S. government, personal information may not be disseminated solely because the individual concerned is a non-U.S. person and "signals intelligence about the routine activities of a foreign person would not be considered foreign intelligence that could be disseminated or retained permanently by virtue of that fact alone unless it is otherwise responsive to an authorized foreign intelligence requirement."[98]

---

[93] According to the ODNI Representations, these restrictions apply regardless of whether the information was collected in bulk or through targeted collection, and of the individual's nationality.

[94] See ODNI Representations (Annex VI).

[95] See Sec. 4(a)(i) of PPD-28 with Sec 2.3 of E.O. 12333.

[96] Sec. 4(a)(i) of PPD-28; ODNI Representations (Annex VI), p. 7. For instance, for personal information collected under Sec. 702 FISA, the NSA's FISC-approved minimization procedures foresee as a rule that the metadata and unevaluated content for PRISM is retained for no more than five years, whereas UPSTREAM data is retained for no more than two years. The NSA complies with these storage limits through an automated process that deletes collected data at the end of the respective retention period. See NSA Sec. 702 FISA Minimization Procedures, Sec. 7 with Sec. 6(a)(1); NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014. Likewise, retention under Sec. 501 FISA (ex-Sec. 215 U.S. PATRIOT ACT) is limited to five years, unless the personal data form part of properly approved dissemination of foreign intelligence information or the DOJ advises the NSA in writing that the records are subject to a preservation obligation in pending or anticipated litigation. See NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.01.2016.

[97] In particular, in case of Sec. 501 FISA (ex-Sec. 215 U.S. PATRIOT ACT), dissemination of personal information may take place only for counterterrorism purposes or as evidence of a crime; in case of Sec. 702 FISA only if there is a valid foreign intelligence or law enforcement purpose. Cf. NSA, CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014; Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.01.2016. See also NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014.

[98] ODNI Representations (Annex VI), p. 7 (with reference to Intelligence Community Directive (ICD) 203).

(88) On the basis of all of the above, the Commission concludes that there are rules in place in the United States designed to limit any interference for national security purposes with the fundamental rights of the persons whose personal data are transferred from the Union to the United States under the EU-U.S. Privacy Shield to what is strictly necessary to achieve the legitimate objective in question.

(89) As the above analysis has shown, U.S. law ensures that surveillance measures will only be employed to obtain foreign intelligence information – which is a legitimate policy objective[99] – and be tailored as much as possible. In particular, bulk collection will only be authorised exceptionally where targeted collection is not feasible, and will be accompanied by additional safeguards to minimise the amount of data collected and subsequent access (which will have to be targeted and only be allowed for specific purposes).

(90) In the Commission's assessment, this conforms with the standard set out by the Court of Justice in the *Schrems* judgment, according to which legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must impose "minimum safeguards"[100] and "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."[101] Neither will there be unlimited collection and storage of data of all persons without any limitations, nor unlimited access. Moreover, the representations provided to the Commission, including the assurance that U.S. signals intelligence activities touch only a fraction of the communications traversing the Internet, exclude that there would be access "on a generalised basis" to the content of electronic communications.[102]

3.1.2. Effective legal protection

(91) The Commission has assessed both the oversight mechanisms that exist in the United States with regard to any interference by U.S. intelligence authorities with personal

---

[99] The Court of Justice has clarified that national security constitutes a legitimate policy objective. See *Schrems*, paragraph 88. See also *Digital Rights Ireland and Others*, paragraphs 42-44 and 51, in which the Court of Justice considered that the fight against serious crime, in particular organised crime and terrorism, may depend to a large extent on the use of modern investigation techniques. Moreover, unlike for criminal investigations that typically concern the retrospective determination of responsibility and guilt for past conduct, intelligence activities often focus on preventing threats to national security before harm has occurred. Therefore, such investigations may often have to cover a broader range of possible actors ("targets") and a wider geographic area. Cf. ECtHR, *Weber and Saravia v. Germany*, Decision of 29.06.2006, Application no. 54934/00, paragraphs 105-118 (on so-called "strategic monitoring").

[100] *Schrems*, paragraph 91, with further references.

[101] *Schrems*, paragraph 93.

[102] Cf. *Schrems*, paragraph 94.

data transferred to the United States and the avenues available for EU data subjects to seek individual redress.

Oversight

(92) The U.S. intelligence community is subject to various review and oversight mechanisms that fall within the three branches of the State. These include internal and external bodies within the executive branch, a number of Congressional Committees, as well as judicial supervision the latter specifically with respect to activities under the Foreign Intelligence Surveillance Act.

(93) First, intelligence activities by U.S. authorities are subject to extensive oversight from within the executive branch.

(94) According to PPD-28, Section 4(a)(iv), the policies and procedures of Intelligence Community elements "shall include appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information"; these measures should include periodic auditing.[103]

(95) Multiple oversight layers have been put in place in this respect, including civil liberties or privacy officers, Inspector Generals, the ODNI Civil Liberties and Privacy Office, the PCLOB, and the President's Intelligence Oversight Board. These oversight functions are supported by compliance staff in all the agencies.[104]

(96) As explained by the U.S. government[105], *civil liberties or privacy officers* with oversight responsibilities exist at various departments with intelligence responsibilities and intelligence agencies.[106] While the specific powers of these officers may vary somewhat depending on the authorising statute, they typically encompass the supervision of procedures to ensure that the respective department/agency is adequately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints from individuals who consider that their privacy or civil liberties have been violated (and in some cases, like the ODNI, may themselves have the power to investigate complaints[107]). The head of the department/ agency in turn has to ensure that the officer receives all the information and is given access to all material necessary to carry out his functions. Civil liberties and privacy officers periodically report to Congress and the PCLOB, including on the number and

---

[103] ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, p. 7. See e.g. CIA, Signals Intelligence Activities, p. 6 (Compliance); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III (A)(4), (B)(4); NSA, PPD-28 Section 4 Procedures, 12.01.2015, Sec. 8.1, 8.6(c).

[104] For instance, the NSA employs more than 300 compliance staff in the Directorate for Compliance. See ODNI Representations (Annex VI), p. 7.

[105] See Ombudsperson Mechanism (Annex III), Sec. 6(b) (i) to (iii).

[106] See 42 U.S.C. § 2000ee-1. This includes for instance the Department of State, the Department of Justice (including the FBI), the Department of Homeland Security, the Department of Defense, the NSA, CIA and the ODNI.

[107] According to the U.S. government, if the ODNI Civil Liberties and Privacy Office receives a complaint, it will also coordinate with other Intelligence Community elements on how that complaint should be further processed within the IC. See Ombudsperson Mechanism (Annex III), Sec. 6(b) (ii).

nature of the complaints received by the department/agency and a summary of the disposition of such complaints, the reviews and inquiries conducted and the impact of the activities carried out by the officer.[108] According to the assessment by the national data protection authorities, the internal oversight exercised by the civil liberties or privacy officers can be considered as "fairly robust", even though in their view they do not meet the required level of independence.[109]

(97) In addition, each Intelligence Community element has its own *Inspector General* with responsibility, among others, to oversee foreign intelligence activities.[110] This includes, within the ODNI, an Office of the Inspector General with comprehensive jurisdiction over the entire Intelligence Community and authorised to investigate complaints or information concerning allegations of unlawful conduct, or abuse of authority, in connection with ODNI and/or Intelligence Community programs and activities.[111] Inspectors General are statutorily independent[112] units responsible for conducting audits and investigations relating to the programs and operations carried out by the respective agency for national intelligence purposes, including for abuse or violation of the law.[113] They are authorised to have access to all records, reports, audits, reviews, documents, papers, recommendations or other relevant material, if need be by subpoena, and may take testimony.[114] While the Inspectors General can only issue non-binding recommendations for corrective action, their reports, including

---

[108] See 42 U.S.C. § 2000ee-1 (f)(1),(2).

[109] Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (adopted 13.4.2016), p. 41.

[110] ODNI Representations (Annex VI), p. 7. See e.g. NSA, PPD-28 Section 4 Procedures, 12.01.2015, Sec. 8.1; CIA, Signals Intelligence Activities, p. 7 (Responsibilities).

[111] This Inspector General (IG) (which was created in October 2010) is appointed by the President, with Senate confirmation, and can be removed only by the President, not the DNI.

[112] These IGs have secure tenure and may only be removed by the President who must communicate to Congress in writing the reasons for any such removal. This does not necessarily mean that they are completely free from instructions. In some cases, the head of the department may prohibit the Inspector General from initiating, carrying out, or completing an audit or investigation where this is considered necessary to preserve important national (security) interests. However, Congress must be informed of the exercise of this authority and on this basis could hold the respective director responsible. See, e.g., Inspector General Act of 1978, § 8 (IG of the Department of Defense); § 8E (IG of the DOJ), § 8G (d)(2)(A),(B) (IG of the NSA); 50. U.S.C. § 403q (b) (IG for the CIA); Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f) (IG for the Intelligence Community). According to the assessment by the national data protection authorities, the Inspector-Generals "*are likely to meet the criterion for organisational independence as defined by the CJEU and the European Court of Human Rights (ECtHR), at least from the moment the new nomination process applies to all*." See Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (adopted 13.4.2016), p. 40.

[113] See ODNI Representations (Annex VI), p. 7. See also Inspector General Act of 1978, as amended, Pub. L. 113-126 of 7.07.2014.

[114] See Inspector General Act of 1978, § 6.

on follow-up action (or the lack thereof) are made public and moreover sent to Congress which can on this basis exercise its oversight function.[115]

(98) Furthermore, the *Privacy and Civil Liberties Oversight Board*, an independent agency[116] within the executive branch composed of a bipartisan, five-member Board[117] appointed by the President for a fixed six-year term with Senate approval, is entrusted with responsibilities in the field of counterterrorism policies and their implementation, with a view to protect privacy and civil liberties. In its review of Intelligence Community action, it may access all relevant agency records, reports, audits, reviews, documents, papers and recommendations, including classified information, conduct interviews and hear testimony. It receives reports from the civil liberties and privacy officers of several federal departments/agencies[118], may issue recommendations to them, and regularly reports to Congressional committees and the President.[119] The PCLOB is also tasked, within the confines of its mandate, to prepare a report assessing the implementation of PPD-28.

(99) Finally, the aforementioned oversight mechanisms are complemented by the *Intelligence Oversight Board* established within the President's Intelligence Advisory Board which oversees compliance by U.S. intelligence authorities with the Constitution and all applicable rules.

(100) To facilitate the oversight, Intelligence Community elements are encouraged to design information systems to allow for the monitoring, recording and reviewing of queries or other searches of personal information.[120] Oversight and compliance bodies will periodically check the practices of Intelligence Community elements for protecting personal information contained in signals intelligence and their compliance with those procedures.[121]

(101) These oversight functions are moreover supported by extensive reporting requirements with respect to non-compliance. In particular, agency procedures must ensure that, when a significant compliance issue occurs involving personal information of any

---

[115] See ODNI Representations (Annex VI), p. 7. See also Inspector General Act of 1978, §§ 4(5), 5. According to Sec. 405(b)(3),(4) of the Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111-259 of 7.10.2010, the IG for the Intelligence Community will keep the DNI as well as Congress informed of the necessity for, and the progress of, corrective actions.

[116] According to the assessment by the national data protection authorities, the PCLOB has in the past "demonstrated its independent powers". See Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (adopted 13.4.2016), p. 42.

[117] In addition, the PCLOB employs some 20 regular staff. See https://www.pclob.gov/about-us/staff.html.

[118] These include at least the Department of Justice, the Department of Defense, the Department of Homeland Security, the Director of National Intelligence and the Central Intelligence Agency, plus any other department, agency or element of the executive branch designated by the PCLOB to be appropriate for coverage.

[119] See 42 U.S.C. § 2000ee. See also Ombudsperson Mechanism (Annex III), Sec. 6(b) (iv). Among others, the PCLOB is required to report when an Executive Branch agency declines to follow its advice.

[120] ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, pp. 7-8.

[121] Id. at p. 8. See also ODNI Representations (Annex VI), p. 9.

person, regardless of nationality, collected through signals intelligence, such issue shall be promptly reported to the head of the Intelligence Community element, which in turn will notify the Director of National Intelligence who, under PPD-28, shall determine if any corrective actions are necessary.[122] Moreover, according to E.O. 12333, all Intelligence Community elements are required to report to the Intelligence Oversight Board on non-compliance incidents.[123] These mechanisms ensure that the issue will be addressed at the highest level in the Intelligence Community. Where it involves a non-U.S. person, the Director of National Intelligence, in consultation with the Secretary of State and the head of the notifying department or agency, shall determine whether steps should be taken to notify the relevant foreign government, consistent with the protection of sources and methods and of U.S. personnel.[124]

(102) Second, in addition to these oversight mechanisms within the executive branch, the U.S. Congress, specifically the *House and Senate Intelligence and Judiciary Committees*, have oversight responsibilities regarding all U.S. foreign intelligence activities, including U.S. signals intelligence. According to the National Security Act, "[t]he President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this subchapter."[125] Also, "[t]he President shall ensure that any illegal intelligence activity is reported promptly to the congressional intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity."[126] Members of these committees have access to classified information as well as intelligence methods and programs.[127]

(103) Later statutes have extended and refined the reporting requirements, both regarding the Intelligence Community elements, the relevant Inspector Generals and the Attorney-General. For instance, FISA requires the Attorney General to "fully inform" the Senate and House Intelligence and Judiciary Committees regarding the government's activities under certain sections of FISA.[128] It also requires the government to provide the Congressional committees with "copies of all decisions, orders, or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation" of FISA provisions. In

---

122 ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, p. 7. See, e.g., NSA, PPD-28 Section 4 Procedures, 12.01.2015, Sec. 7.3, 8.7(c),(d); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III.(A)(4), (B)(4); CIA, Signals Intelligence Activities, p. 6 (Compliance) and p. 8 (Responsibilities).

123 See E.O. 12333, Sec. 1.6(c).

124 PPD-28, Sec. 4(a)(iv).

125 See Sec. 501(a)(1) (50 U.S.C. § 413(a)(1)). This provision contains the general requirements as regards Congressional oversight in the area of national security.

126 See Sec. 501(b) (50 U.S.C. § 413(b)).

127 Cf. Sec. 501(d) (50 U.S.C. § 413(d)).

128 See 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

particular, as regards surveillance under Section 702 FISA, oversight is exercised through statutorily required reports to the Intelligence and Judiciary Committees, as well as frequent briefings and hearings. These include a semi-annual report by the Attorney General describing the use of Section 702 FISA, with supporting documents including notably the Department of Justice and ODNI compliance reports and a description of any incidents of non-compliance,[129] and a separate semi-annual assessment by the Attorney General and the DNI documenting compliance with the targeting and minimization procedures, including compliance with the procedures designed to ensure that collection is for a valid foreign intelligence purpose.[130] Congress also receives reports by the Inspector Generals who are authorised to evaluate the agencies' compliance with targeting and minimization procedures and Attorney General Guidelines.

(104) According to the USA FREEDOM Act of 2015, the U.S. government must disclose to Congress (and the public) each year the number of FISA orders and directives sought and received, as well as estimates of the number of U.S. and non-U.S. persons targeted by surveillance, among others.[131] The Act also requires additional public reporting about the number of NSL issued, again both with regard to U.S. and non-U.S. persons (while at the same time allowing the recipients of FISA orders and certifications, as well as NSL requests, to issue transparency reports under certain conditions).[132]

(105) Third, intelligence activities by U.S. public authorities based on FISA allow for review, and in some cases prior authorisation of the measures, by the *FISA Court* (FISC)[133], an independent tribunal[134] whose decisions can be challenged before the Foreign Intelligence Court of Review (FISCR)[135] and, ultimately, the Supreme Court

---

129 See 50 U.S.C. § 1881f.

130 See 50 U.S.C. § 1881a(l)(1).

131 See USA FREEDOM Act of 2015, Pub. L. No. 114-23, Sec. 602(a). In addition, according to Sec 402, "the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term 'specific selection term', and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion."

132 USA FREEDOM Act, Sec. 602(a), 603(a).

133 For certain types of surveillance, alternatively a U.S. Magistrate Judge publicly designated by the Chief Justice of the United States may have the power to hear applications and grant orders.

134 The FISC is comprised of eleven judges appointed by the Chief Justice of the United States from among sitting U.S. district court judges, who previously have been appointed by the President and confirmed by the Senate. The judges, who have life tenure and can only be removed for good cause, serve on the FISC for staggered seven-year terms. FISA requires that the judges be drawn from at least seven different U.S. judicial circuits. See Sec 103 FISA (50 U.S.C. 1803 (a)); PCLOB, Sec. 215 Report, pp. 174-187. The judges are supported by experienced judicial law clerks that constitute the court's legal staff and prepare legal analysis on collection requests. See PCLOB, Sec. 215 Report, p. 178; Letter from the Honourable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to the Honourable Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate (July 29, 2013) ("Walton Letter"), pp. 2-3.

135 The FISCR is composed of three judges appointed by the Chief Justice of the United States and drawn from U.S. district courts or courts of appeals, serving for a staggered seven year term. See Sec. 103 FISA (50 U.S.C. § 1803 (b)).

of the United States.[136] In case of prior authorisation, the requesting authorities (FBI, NSA, CIA, etc.) will have to submit a draft application to lawyers at the National Security Department of the Department of Justice who will scrutinise it and, if necessary, request additional information.[137] Once the application has been finalised, it will have to be approved by the Attorney General, Deputy Attorney General or the Assistant Attorney General for National Security.[138] The Department of Justice will then submit the application to the FISC that will assess the application and make a preliminary determination on how to proceed.[139] Where a hearing takes place, the FISC has the authority to take testimony which may include expert advice.[140]

(106) The FISC (and FISCR) is supported by a standing panel of five individuals that have an expertise in national security matters as well as civil liberties.[141] From this group the court shall appoint an individual to serve as *amicus curiae* to assist in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court finds that such appointment is not appropriate.[142] This shall in particular ensure that privacy considerations are properly reflected in the court's assessment. The court may also appoint an individual or organisation to serve as *amicus curiae*, including providing technical expertise, whenever it deems this appropriate or, upon motion, permit an individual or organisation leave to file an *amicus curiae* brief.[143]

(107) As regards the two legal authorisations for surveillance under FISA that are most important for data transfers under the EU-U.S. Privacy Shield, oversight by the FISC differs.

---

136 See 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

137 For instance, additional factual details about the target of the surveillance, technical information about the surveillance methodology, or assurances about how the information acquired will be used and disseminated. See PCLOB, Sec. 215 Report, p. 177.

138 50 U.S.C. §§ 1804 (a), 1801 (g).

139 The FISC may approve the application, request further information, determine the necessity of a hearing or indicate a possible denial of the application. On the basis of this preliminary determination, the government will make its final application. The latter may include substantial changes to the original application on the basis of the judge's preliminary comments. Although a large percentage of final applications are approved by the FISC, a substantial part of these contain substantive changes to the original application, e.g. 24% of applications approved for the period from July to September 2013. See PCLOB, Sec. 215 Report, p.179; Walton Letter, p. 3.

140 PCLOB, Sec. 215 Report, p.179, n. 619.

141 50 U.S.C. § 1803 (i)(1),(3)(A). This new legislation implemented recommendations by the PCLOB to establish a pool of privacy and civil liberties experts that can serve as *amicus curiae*, in order to provide the court with legal arguments to the advancement of privacy and civil liberties. See PCLOB, Sec. 215 Report, pp. 183-187.

142 50 U.S.C. § 1803 (i)(2)(A). According to information by the ODNI, such appointments have already taken place. See Signals Intelligence Reform, 2016 Progress Report.

143 50 U.S.C. § 1803 (i)(2)(B).

(108) Under Section 501 FISA[144], which allows the collection of "any tangible things (including books, records, papers, documents, and other items)", the application to the FISC must contain a statement of facts showing that there are reasonable grounds to believe that the tangible things sought for are relevant to an authorised investigation (other than a threat assessment) conducted to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. Also, the application must contain an enumeration of the minimisation procedures adopted by the Attorney General for the retention and dissemination of the collected intelligence. [145]

(109) Conversely, under Section 702 FISA[146], the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence. Section 702 FISA allows the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.[147] Such targeting is carried out by the NSA in two steps: First, NSA analysts will identify non-U.S. persons located abroad whose surveillance will lead, based on the analysts' assessment, to the relevant foreign intelligence specified in the certification. Second, once these individualised persons have been identified and their targeting has been approved by an extensive review mechanism within the NSA[148], selectors identifying communication facilities (such as email addresses) used by the targets will be "tasked" (i.e. developed and applied).[149] As indicated, the certifications to be approved by the FISC contain no information about the individual persons to be targeted but rather identify categories of foreign intelligence information.[150] While the FISC does not assess – under a probable cause or any other standard – that individuals are properly targeted to acquire foreign intelligence information,[151] its control extends to the condition that "a significant purpose of the acquisition is to obtain foreign intelligence information"[152]. Indeed, under Section 702 FISA, the NSA is allowed to collect communications of non-U.S. persons outside the U.S. only if it can be reasonably believed that a given means of communication is being used to communicate foreign intelligence information (e.g. related to international terrorism, nuclear proliferation or hostile cyber activities).

---

144 50 U.S.C. § 1861

145 50 U.S.C. § 1861 (b).

146 50 U.S.C. § 1881.

147 50 U.S.C. § 1881a (a).

148 PCLOB, Sec. 702 Report, p. 46.

149 50 U.S.C. § 1881a (h).

150 50 U.S.C. § 1881a (g). According to the PCLOB, these categories have so far mainly concerned international terrorism and topics such as the acquisition of weapons of mass destruction. See PCLOB, Sec. 702 Report, p. 25.

151 PCLOB, Sec. 702 Report, p. 27.

152 50 U.S.C. § 1881a.

Determinations to this effect are subject to judicial review.[153] Certifications also need to provide for targeting and minimization procedures.[154] The Attorney General and the Director of National Intelligence verify compliance and the agencies have the obligation to report any incidents of non-compliance to the FISC[155] (as well as the Congress and the President's Intelligence Oversight Board), which on this basis can modify the authorisation.[156]

(110) Furthermore, to increase the efficiency of the oversight by the FISC, the U.S. Administration has agreed to implement a recommendation by the PCLOB to supply to the FISC documentation of Section 702 targeting decisions, including a random sample of tasking sheets, so as to allow the FISC to assess how the foreign intelligence purpose requirement is being met in practice.[157] At the same time, the U.S. Administration accepted and has taken measures to revise NSA targeting procedures to better document the foreign intelligence reasons for targeting decisions.[158]

Individual redress

(111) A number of avenues are available under U.S. law to EU data subjects if they have concerns whether their personal data have been processed (collected, accessed, etc.) by U.S. Intelligence Community elements, and if so, whether the limitations applicable in U.S. law have been complied with. These relate essentially to three areas: interference under FISA; unlawful, intentional access to personal data by government officials; and access to information under Freedom of Information Act (FOIA).[159]

---

153 "Liberty and Security in a Changing World", Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 12.12.2013, p. 152.

154 50 U.S.C.1881a (i).

155 Rule 13(b) of the FISC Rules of Procedure requires the government to file a written notice with the Court immediately upon discovering that any authority or approval granted by the Court has been implemented in a manner that does not comply with the Court's authorization or approval, or with applicable law. It also requires the government to notify the Court in writing of the facts and circumstances relevant to such non-compliance. Typically, the government will file a final Rule 13(a) notice once the relevant facts are known and any unauthorized collection has been destroyed. See Walton Letter, p. 10.

156 50 U.S.C. § 1881 (l). See also PCLOB, Sec. 702 Report, pp. 66-76; NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014. The collection of personal data for intelligence purposes under Sec 702 FISA is subject to both internal and external oversight within the executive branch. Among others, the internal oversight includes internal compliance programs to evaluate and oversee compliance with targeting and minimization procedures; reporting of non-compliance incidents, both internally and externally to the ODNI, Department of Justice, Congress and the FISC; and annual reviews sent to the same bodies. As for external oversight, it mainly consists in targeting and minimization reviews conducted by the ODNI, DOJ and Inspectors General, which in turn report to Congress and the FISC, including on non-compliance incidents. Significant compliance incidents must be reported to the FISC immediately, others in a quarterly report. See PCLOB, Sec. 702 Report, pp. 66-77.

157 PCLOB, Recommendations Assessment Report, 29.01.2015, p. 20.

158 PCLOB, Recommendations Assessment Report, 29.01.2015, p. 16.

159 In addition, Sec. 10 of the Classified Information Procedures Act provides that, in any prosecution in which the United States must establish that material constitutes classified information (e.g. because it requires protection against unauthorized disclosure for reasons of national security), the United States shall notify the defendant of the portions of the material that it reasonably expects to rely upon to establish the classified information element of the offense.

(112) First, the Foreign Intelligence Surveillance Act provides a number of remedies, available also to non-U.S. persons, to challenge unlawful electronic surveillance.[160] This includes the possibility for individuals to bring a civil cause of action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed;[161] to sue U.S. government officials in their personal capacity ("under colour of law") for money damages;[162] and to challenge the legality of surveillance (and seek to suppress the information) in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the United States.[163]

(113) Second, the U.S. government referred the Commission to a number of additional avenues that EU data subjects could use to seek legal recourse against government officials for unlawful government access to, or use of, personal data, including for purported national security purposes (i.e. the Computer Fraud and Abuse Act;[164] Electronic Communications Privacy Act;[165] and Right to Financial Privacy Act[166]). All of these causes of action concern specific data, targets and/or types of access (e.g. remote access of a Computer via the Internet) and are available under certain conditions (e.g. intentional/wilful conduct, conduct outside of official capacity, harm suffered).[167] A more general redress possibility is offered by the Administrative Procedure Act (5 U.S.C. § 702), according to which "any person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action", is entitled to seek judicial review. This includes the possibility to ask the court to "hold unlawful and set aside agency action, findings, and conclusions found to be […] arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law".[168]

(114) Finally, the U.S. government has pointed to the FOIA as a means for non-U.S. persons to seek access to existing federal agency records, including where these contain the individual's personal data.[169] Given its focus, the FOIA does not provide an avenue for individual recourse against interference with personal data as such, even though it could in principle enable individuals to get access to relevant information held by national intelligence agencies. Even in this respect the possibilities appear to be

---

160 See for the following ODNI Representations (Annex VI), p. 16.

161 18 U.S.C. § 2712.

162 50 U.S.C. § 1810.

163 50 U.S.C. § 1806.

164 18 U.S.C. § 1030.

165 18 U.S.C. §§ 2701-2712.

166 12 U.S.C. § 3417.

167 ODNI Representations (Annex VI), p. 17.

168 5 U.S.C. § 706(2)(A).

169 5 U.S.C. § 552. Similar laws exist at State level.

limited as agencies may withhold information that falls within certain enumerated exceptions, including access to classified national security information and information concerning law enforcement investigations.[170] This being said, the use of such exceptions by national intelligence agencies can be challenged by individuals who can seek both administrative and judicial review.

(115) While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available causes of action are limited[171] and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show "standing"[172], which restricts access to ordinary courts.[173]

(116) In order to provide for an additional redress avenue accessible for all EU data subjects, the U.S. government has decided to create a new Ombudsperson Mechanism as set out in the letter from the U.S. Secretary of State to the Commission which is contained in Annex III to this decision. This mechanism builds on the designation, under PPD-28, of a Senior Coordinator (at the level of Under-Secretary) in the State Department as a contact point for foreign governments to raise concerns regarding U.S. signals intelligence activities, but goes significantly beyond this original concept.

(117) In particular, according to the commitments from the U.S. government, the Ombudsperson Mechanism will ensure that individual complaints are properly investigated and addressed, and that individuals receive independent confirmation that U.S. laws have been complied with or, in case of a violation of such laws, the non-compliance has been remedied.[174] The Mechanism includes "the Privacy Shield Ombudsperson", i.e. the Under-Secretary and further staff as well as other oversight bodies competent to oversee the different elements of the Intelligence Community on

---

[170] If this is the case, the individual will normally only receive a standard reply by which the agency declines either to confirm or deny the existence of any records. See *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

[171] See ODNI Representations (Annex VI), p. 16. According to the explanations provided, the available causes of action either require the existence of *damage* (18 U.S.C. § 2712; 50 U.S.C. § 1810) or a showing that the *government intends to use or disclose information* obtained or derived from electronic surveillance of the person concerned against that person *in judicial or administrative proceedings* in the United States (50 U.S.C. § 1806). However, as the Court of Justice has repeatedly stressed, to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the person concerned has suffered any adverse consequences on account of that interference. See *Schrems*, paragraph 89 with further references.

[172] This admissibility criterion stems from the 'case or controversy' requirement of the U.S. Const., Art. III.

[173] See *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013). As regards the use of NSLs, the USA FREEDOM Act (Sec. 502(f)-503) provides that non-disclosure requirements must be periodically reviewed, and that *recipients* of NSL be notified when the facts no longer support a non-disclosure requirement (see ODNI Representations (Annex VI), p. 13). However, this does not ensure that the EU data subject would be informed that (s)he has been the target of an investigation.

[174] In case the complainant seeks access to documents held by U.S. public authorities, the rules and procedures set out in the Freedom of Information Act apply. This includes the possibility to seek judicial redress (rather than independent oversight) in case the request is rejected, under the conditions set out in the FOIA.

whose cooperation the Privacy Shield Ombudsperson will rely in dealing with complaints. In particular, where an individual's request relates to the compatibility of surveillance with U.S. law, the Privacy Shield Ombudsperson will be able to rely on independent oversight bodies with investigatory powers (such as the Inspector-Generals or the PCLOB). In each case the Secretary of State ensures that the Ombudsperson will have the means to ensure that its response to individual requests is based on all the necessary information.

(118) Through this 'composite structure', the Ombudsperson Mechanism guarantees independent oversight and individual redress. Moreover, the cooperation with other oversight bodies ensures access to the necessary expertise. Finally, by imposing an obligation on the Privacy Shield Ombudsperson to confirm compliance or remediation of any non-compliance, the mechanism reflects a commitment from the U.S. government as a whole to address and resolve complaint from EU individuals.

(119) First, differently from a pure government-to-government mechanism, the Privacy Shield Ombudsperson will receive and respond to individual complaints. Such complaints can be addressed to the supervisory authorities in the Member States competent for the oversight of national security services and/or the processing of personal data by public authorities that will submit them to a centralised EU body from where they will be channelled to the Privacy Shield Ombudsperson.[175] This will in fact benefit EU individuals who can turn to a national authority 'close to home' and in their own language. It will be the task of such an authority to support the individual in making a request to the Privacy Shield Ombudsperson that contains the basic information and thus can be considered "complete". The individual does not have to demonstrate that his/her personal data have in fact been accessed by the U.S. government through signals intelligence activities.

(120) Second, the U.S. government commits to ensure that, in carrying out its functions, the Privacy Shield Ombudsperson will be able to rely on the cooperation from other oversight and compliance review mechanisms existing in U.S. law. This will sometimes involve national intelligence authorities, in particular where the request is to be interpreted as one for access to documents under the Freedom of Information Act. In other cases, particularly when requests relate to the compatibility of surveillance with U.S. law, such cooperation will involve independent oversight bodies (e.g. Inspector Generals) with the responsibility and power to carry out a thorough investigation (in particular through access to all relevant documents and the power to request information and statements) and address non-compliance.[176] Also, the Privacy Shield Ombudsperson will be able to refer matters to the PCLOB for its

[175] According to the Ombudsperson Mechanism (Annex III), Sec. 4(f), the Privacy Shield Ombudsperson will communicate directly with the EU individual complaint handling body, who will in turn be responsible for communicating with the individual submitting the request. If direct communications are part of the "underlying processes" that may provide the requested relief (e.g. a FOIA access request, see Sec. 5), those communications will take place in accordance with the applicable procedures.

[176] See Ombudsperson Mechanism (Annex III), Sec. 2(a). See also recitals (96)-(97).

consideration.[177] Where any non-compliance has been found by one of these oversight bodies, the Intelligence Community element (e.g. an intelligence agency) concerned will have to remedy the non-compliance as only this will allow the Ombudsperson to provide a "positive" response to the individual (i.e. that any non-compliance has been remedied) to which the U.S. government has committed. Also, as part of the cooperation, the Privacy Shield Ombudsperson will be informed of the outcome of the investigation, and the Ombudsperson will have the means to ensure that it receives all the information necessary to prepare its response.

(121) Finally, the Privacy Shield Ombudsperson will be independent from, and thus free from instructions by, the U.S. Intelligence Community.[178] This is of significant importance, given that the Ombudsperson will have to "confirm" that (i) the complaint has been properly investigated and that (ii) relevant U.S. law – including in particular the limitations and safeguards set out in Annex VI – has been complied with or, in the event of non-compliance, such violation has been remedied. In order to be able to provide that independent confirmation, the Privacy Shield Ombudsperson will have to receive the necessary information regarding the investigation to assess the accuracy of the response to the complaint. In addition, the Secretary of State has committed to ensure that the Under-Secretary will carry out the function as Privacy Shield Ombudsperson objectively and free from any improper influence liable to have an effect on the response to be provided.

(122) Overall, this mechanism ensures that individual complaints will be thoroughly investigated and resolved, and that at least in the field of surveillance this will involve independent oversight bodies with the necessary expertise and investigatory powers and an Ombudsperson that will be able to carry out its functions free from improper, in particular political, influence. Moreover, individuals will be able to bring complaints without having to demonstrate, or just to provide indications, that they have been the object of surveillance.[179] In the light of these features, the Commission is satisfied that there are adequate and effective guarantees against abuse.

(123) On the basis of all the above, the Commission concludes that the United States ensures effective legal protection against interferences by its intelligence authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the EU-U.S. Privacy Shield.

---

[177] See Ombudsperson Mechanism (Annex III), Sec. 2(c). According to the explanations provided by the U.S. government, the PCLOB shall continually review the policies and procedures, as well as their implementation, of those U.S. authorities responsible for counterterrorism to determine whether their actions "appropriately protect privacy and civil liberties and are consistent with governing laws, regulations, and policies regarding privacy and civil liberties." It also shall "receive and review reports and other information from privacy officers and civil liberties officers and, when appropriate, make recommendations to them regarding their activities."

[178] See *Roman Zakharov v. Russia*, Judgment of 4.12.2015 (Grand Chamber), Application No. 47143/06, paragraph 275 ("although it is in principle desirable to entrust supervisory control to a judge, supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance and is vested with sufficient and effective oversight powers").

[179] See *Kennedy v. the United Kingdom*, Judgment of 18.5.2010, Application No. 26839/05, paragraph 167.

(124) In this respect, the Commission takes note of the Court of Justice's judgment in the *Schrems* case according to which "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification of erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter."[180] The Commission's assessment has confirmed that such legal remedies are provided for in the United States, including through the introduction of the Ombudsperson mechanism. The Ombudsperson mechanism provides for independent oversight with investigatory powers. In the framework of the Commission's continuous monitoring of the Privacy Shield, including through the annual joint review which shall also involve the Ombudsperson, the effectiveness of this mechanism will be reassessed.

3.2. Access and use by U.S. public authorities for law enforcement and public interest purposes

(125) As regards interference with personal data transferred under the EU-U.S. Privacy Shield for law enforcement purposes, the U.S. government (through the Department of Justice) has provided assurance on the applicable limitations and safeguards which in the Commission's assessment demonstrate an adequate level of protection.

(126) According to this information, under the Fourth Amendment of the U.S. Constitution[181] searches and seizures by law enforcement authorities principally[182] require a court-ordered warrant upon a showing of "probable cause". In the few specifically established and exceptional cases where the warrant requirement does not apply[183], law enforcement is subject to a "reasonableness" test.[184] Whether a search or seizure is reasonable is "determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is

---

[180] *Schrems*, paragraph 95. As is clear from paragraphs 91, 96 of the judgment, paragraph 95 concerns the level of protection guaranteed in the Union legal order, to which the level of protection in the third country must be "essentially equivalent". According to paragraphs 73 and 74 of the judgment, this does not require that the level of protection or the means to which the third country has recourse must be identical, even though the means to be employed have to prove, in practice, effective.

[181] According to the Fourth Amendment, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Only (magistrate) judges may issue search warrants. Federal warrants for the copying of electronically stored information are further governed by Rule 41 of the Federal Rules of Criminal Procedure.

[182] Repeatedly, the Supreme Court has referred to searches without warrants as "exceptional". See e.g. *Johnson v. United States*, 333 U.S. 10, 14 (1948); *McDonald v. United States*, 335 U.S. 451, 453 (1948); *Camara v. Municipal Court*, 387 U.S. 523, 528-29 (1967); *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 352-53, 355 (1977). Likewise, the Supreme Court regularly stresses that "the most basic constitutional rule in this area is that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment−subject only to a few specifically established and well-delineated exceptions." See e.g. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971); *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 352-53, 358 (1977).

[183] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).

[184] PCLOB, Sec. 215 Report, p. 107, referring to *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).

needed for the promotion of legitimate governmental interests."[185] More generally, the Fourth Amendment guarantees privacy, dignity, and protects against arbitrary and invasive acts by officers of the Government.[186] These concepts capture the idea of necessity and proportionality in Union law. Once law enforcement no longer has a need to use the seized items as evidence, they should be returned.[187]

(127) While the Fourth Amendment right does not extend to non-U.S. persons that are not resident in the United States, the latter nevertheless benefit indirectly from its protections, given that the personal data are held by U.S. companies with the effect that law enforcement authorities in any event have to seek judicial authorisation (or at least respect the reasonableness requirement).[188] Further protections are provided by special statutory authorities, as well as the Department of Justice Guidelines, which limit law enforcement access to data on grounds equivalent to necessity and proportionality (e.g. by requiring that the FBI use the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties).[189] According to the representations made by the U.S. government, the same or higher protections apply to law enforcement investigations at State level (with respect to investigations carried out under State laws).[190]

(128) Although a prior judicial authorisation by a court or grand jury (an investigate arm of the court impanelled by a judge or magistrate) is not required in all cases[191], administrative subpoenas are limited to specific cases and will be subject to independent judicial review at least where the government seeks enforcement in court.[192]

---

185 PCLOB, Sec. 215 Report, p.107, referring to *Samson v. California*, 547 U.S. 843, 848 (2006).

186 *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.

187 See e.g. *United Sates v Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).

188 Cf. *Roman Zakharov v. Russia*, Judgment of 4.12.2015 (Grand Chamber), Application No. 47143/06, paragraph 269, according to which "the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception."

189 DOJ Representations (Annex VII), p. 4 with further references.

190 DOJ Representations (Annex VII), n. 2.

191 According to the information the Commission has received, and leaving aside specific areas likely not relevant for data transfers under the EU-U.S. Privacy Shield (e.g. investigations into health care fraud, child abuse or controlled substances cases), this concerns mainly certain authorities under the Electronic Communications Privacy Act (ECPA), namely requests for basic subscriber, session and billing information (18 U.S.C. § 2703(c)(1), (2), e.g. address, type/length of service) and for the content of emails more than 180 days old (18 U.S.C. § 2703(a), (b)). In the latter case, however, the individual concerned has to be notified and thus has the opportunity to challenge the request in court. See also the overview in DOJ, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Ch. 3: The Stored Communications Act, pp. 115-138.

192 According to the representations by the U.S. government, recipients of administrative subpoenas may challenge them in court on the grounds that they are unreasonable, i.e. overboard, oppressive of burdensome. See DOJ Representations (Annex VII), p. 2.

(129) The same applies for the use of administrative subpoenas for public interest purposes. In addition, according to the representations from the U.S. government, similar substantive limitations apply in that agencies may only seek access to data that is relevant to matters falling with their scope of authority and have to respect the standard of reasonableness.

(130) Moreover, U.S. law provides for a number of judicial redress avenues for individuals, against a public authority or one of its officials, where these authorities process personal data. These avenues, which include in particular the Administrative Procedure Act (APA), the Freedom of Information Act (FOIA) and the Electronic Communications Privacy Act (ECPA), are open to all individuals irrespective of their nationality, subject to any applicable conditions.

(131) Generally, under the judicial review provisions of the Administrative Procedure Act,[193] "any person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action", is entitled to seek judicial review.[194] This includes the possibility to ask the court to "hold unlawful and set aside agency action, findings, and conclusions found to be […] arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law".[195]

(132) More specifically, Title II of the Electronic Communications Privacy Act[196] sets forth a system of statutory privacy rights and as such governs law enforcement access to the contents of wire, oral or electronic communications stored by third-party service providers[197]. It criminalises the unlawful (i.e. not authorised by court or otherwise permissible) access to such communications and provides recourse for an affected individual to file a civil action in U.S. federal court for actual and punitive damages as well as equitable or declaratory relief against a government official that has wilfully committed such unlawful acts, or against the United States.

(133) Also, under the Freedom of Information Act (FOIA, 5 U.S.C. § 552), any person has the right to obtain access to federal agency records and, upon exhaustion of administrative remedies, to enforce such right in court, except to the extent that such

---

193 5 U.S.C. § 702.

194 Generally, only "final" agency action – rather than "preliminary, procedural, or intermediate" agency action – is subject to judicial review. See 5 U.S.C. § 704.

195 5 U.S.C. § 706(2)(A).

196 18 U.S.C. §§ 2701-2712.

197 The ECPA protects communications held by two defined classes of network service providers, namely providers of: (i) electronic communication services, for instance telephony or email; (ii) remote computing services like computer storage or processing services.

records are protected from public disclosure by an exemption or special law enforcement exclusion.[198]

(134) In addition, several other statutes afford individuals the right to bring suit against a U.S. public authority or official with respect to the processing of their personal data, such as the Wiretap Act[199], the Computer Fraud and Abuse Act[200], the Federal Torts Claim Act[201], the Right to Financial Privacy Act[202], and the Fair Credit Reporting Act.[203]

---

198 These exclusions are, however, framed. For example, according to 5 U.S.C. § 552 (b)(7), FOIA rights are ruled out for "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual." Also, "[w]henever a request is made which involves access to records [the production of which could reasonably be expected to interfere with enforcement proceedings] and− (A) the investigation or proceeding involves a possible violation of criminal law; and (B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section." (5 U.S.C. § 552 (c)(1)).

199 18 U.S.C. §§ 2510 et seq. Under the Wiretap Act (18 U.S.C. § 2520), a person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used may bring a civil action for violation of the Wiretap Act, including under certain circumstances against an individual government official or the United States. For the collection of addressing and other non-content information (e.g. IP address, email to/from address), see also the Pen Registers and Trap and Trace Devices chapter of Title 18 (18 U.S.C. §§ 3121-3127 and, for civil action, § 2707).

200 18 U.S.C. § 1030. Under the Computer Fraud and Abuse Act, a person may bring suit against any person with respect to intentional unauthorised access (or exceeding authorised access) to obtain information from a financial institution, a U.S. government computer system or other specified computer, including under certain circumstances against an individual government official.

201 28 U.S.C. §§ 2671 et seq. Under the Federal Tort Claims Act, a person may bring suit, under certain circumstances, against the United States with respect to "the negligent or wrongful act or omission of any employee of the Government while acting within the scope of his office or employment."

202 12 U.S.C. §§ 3401 et seq. Under the Right to Financial Privacy Act, a person may bring suit, under certain circumstances, against the United States with respect to the obtaining or disclosing of protected financial records in violation of the statute. Government access to protected financial records is generally prohibited unless the government makes the request subject to a lawful subpoena or search warrant or, subject to limitations, a formal written request and the individual whose information is sought receives notice of such a request.

203 15 U.S.C. §§ 1681-1681x. Under the Fair Credit Reporting Act, a person may bring suit against any person who fails to comply with requirements (in particular the need for lawful authorisation) regarding the collection, dissemination and use of consumer credit reports, or, under certain circumstances, against a government agency.

(135) The Commission therefore concludes that there are rules in place in the United States designed to limit any interference for law enforcement[204] or other public interest purposes with the fundamental rights of the persons whose personal data are transferred from the Union to the United States under the EU-U.S. Privacy Shield to what is strictly necessary to achieve the legitimate objective in question, and that ensure effective legal protection against such interference.

4. Adequate level of protection under the EU-U.S. Privacy Shield

(136) In the light of the those findings, the Commission considers that the United States ensures an adequate level of protection for personal data transferred from the Union to self-certified organisations in the United States under the EU-U.S. Privacy Shield.

(137) In particular, the Commission considers that the Principles issued by the U.S. Department of Commerce as a whole ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the basic principles laid down in Directive 95/46/EC.

(138) In addition, the effective application of the Principles is guaranteed by the transparency obligations and the administration of the Privacy Shield by the Department of Commerce.

(139) Moreover, the Commission considers that, taken as a whole, the oversight and recourse mechanisms provided for by the Privacy Shield enable infringements of the 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.

(140) Finally, on the basis of the available information about the U.S. legal order, including the representations and commitments from the U.S. government, the Commission considers that any interference by U.S. 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 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.

(141) The Commission concludes that this meets the standards of Article 25 of Directive 95/46/EC, interpreted in light of the Charter of Fundamental Rights of the European Union, as explained by the Court of Justice in particular in the *Schrems* judgment.

5. Action of Data Protection Authorities and information to the Commission

---

[204] The Court of Justice has recognised that law enforcement constitutes a legitimate policy objective. See Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others*, EU:C:2014:238, paragraph 42. See also Article 8(2) ECHR and the judgment by the European Court of Human Rights in *Weber and Saravia v. Germany*, Application no. 54934/00, paragraph 104.

(142) In the *Schrems* judgment, the Court of Justice clarified that the Commission has no competence to restrict the powers that DPAs derive from Article 28 of Directive 95/46/EC (including the power to suspend data transfers) where a person, in bringing a claim under that provision, calls into question the compatibility of a Commission adequacy decision with the protection of the fundamental right to privacy and data protection.[205]

(143) In order to effectively monitor the functioning of the Privacy Shield, the Commission should be informed by Member States about relevant action undertaken by DPAs.

(144) The Court of Justice furthermore considered that, in line with the second subparagraph of Article 25(6) of Directive 95/46/EC, Member States and their organs must take the measures necessary to comply with acts of the Union institutions, as the latter are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality. Consequently, a Commission adequacy decision adopted pursuant to Article 25(6) of Directive 95/46/EC is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities.[206] Where such an authority has received a complaint putting in question the compliance of a Commission adequacy decision with the protection of the fundamental right to privacy and data protection and considers the objections advanced to be well founded, national law must provide it with a legal remedy to put those objections before a national court which, in case of doubts, must stay proceedings and make a reference for a preliminary ruling to the Court of Justice.[207]

6. Periodic review of adequacy finding

(145) In the light of the fact that the level of protection afforded by the U.S. legal order may be liable to change, the Commission, following adoption of this decision, will check periodically whether the findings relating to the adequacy of the level of protection ensured by the United States under the EU-U.S. Privacy Shield are still factually and legally justified. Such a check is required, in any event, when the Commission acquires any information giving rise to a justified doubt in that regard.[208]

(146) Therefore, the Commission will continuously monitor the overall framework for the transfer of personal data created by the EU-U.S. Privacy Shield as well as compliance by U.S. authorities with the representations and commitments contained in the documents attached to this decision. To facilitate this process, the U.S. has committed to inform the Commission of material developments in U.S. law when relevant to the Privacy Shield in the field of data protection and the limitations and safeguards applicable to access to personal data by public authorities. Moreover, this decision will

---

[205] *Schrems*, paragraphs 40 et seq., 101-103.

[206] *Schrems*, paragraphs 51, 52 and 62.

[207] *Schrems*, paragraph 65.

[208] *Schrems*, paragraph 76.

be subject to an Annual Joint Review which will cover all aspects of the functioning of the EU-U.S. Privacy Shield, including the operation of the national security and law enforcement exceptions to the Principles. In addition, since the adequacy finding may also be influenced by legal developments in Union law, the Commission will assess the level of protection provided by the Privacy Shield following the entry into application of the GDPR.

(147) To perform the Annual Joint Review referred to in Annexes I, II and VI, the Commission will meet with the Department of Commerce and FTC, accompanied, if appropriate, by other departments and agencies involved in the implementation of the Privacy Shield arrangements, as well as, for matters pertaining to national security, representatives of the ODNI, other Intelligence Community elements and the Ombudsperson. The participation in this meeting will be open for EU DPAs and representatives of the Article 29 Working Party.

(148) In the framework of the Annual Joint Review, the Commission will request that the Department of Commerce provides comprehensive information on all relevant aspects of the functioning of the EU-U.S. Privacy Shield, including referrals received by the Department of Commerce from DPAs and the results of *ex officio* compliance reviews. The Commission will also seek explanations concerning any questions or matters concerning the EU-U.S. Privacy Shield and its operation arising from any information available, including transparency reports allowed under the USA FREEDOM Act, public reports by U.S. national intelligence authorities, the DPAs, privacy groups, media reports, or any other possible source. Moreover, in order to facilitate the Commission's task in this regard, the Member States should inform the Commission of cases where the actions of bodies responsible for ensuring compliance with the Principles in the United States fail to secure compliance and of any indications that the actions of U.S. public authorities responsible for national security or the prevention, investigation, detection or prosecution of criminal offenses do not ensure the required level of protection.

(149) On the basis of the annual joint review, the Commission will prepare a public report to be submitted to the European Parliament and the Council.

7. Suspension of the adequacy decision

(150) Where, on the basis of the checks or of any other information available, the Commission concludes the level of protection offered by the Privacy Shield can no longer be regarded as essentially equivalent to the one in the Union, or where that there are clear indications that effective compliance with the Principles in the United States might no longer be ensured, or that the actions of U.S. public authorities responsible for national security or the prevention, investigation, detection or prosecution of criminal offenses do not ensure the required level of protection, it will inform the Department of Commerce thereof and request that appropriate measures are taken to swiftly address any potential non-compliance with the Principles within a specified, reasonable timeframe. If, after the expiration of the specified timeframe, the

U.S. authorities fail to demonstrate satisfactorily that the EU-U.S. Privacy Shield continues to guarantee effective compliance and an adequate level of protection, the Commission will initiate the procedure leading to the partial or complete suspension or repeal of this decision.[209] Alternatively, the Commission may propose to amend this decision, for instance by limiting the scope of the adequacy finding only to data transfers subject to additional conditions.

(151) In particular, the Commission will initiate the procedure for suspension or repeal in case of:

(a) indications that the U.S. authorities do not comply with the representations and commitments contained in the documents annexed to this decision, including as regards the conditions and limitations for access by U.S. public authorities for law enforcement, national security and other public interest purposes to personal data transferred under the Privacy Shield;

(b) failure to effectively address complaints by EU data subjects; in this respect, the Commission will take into account all circumstances having an impact on the possibility for EU data subjects to have their rights enforced, including, in particular, the voluntary commitment by self-certified U.S. companies to cooperate with the DPAs and follow their advice; or

(c) failure by the Privacy Shield Ombudsperson to provide timely and appropriate responses to requests from EU data subjects.

(152) The Commission will also consider initiating the procedure leading to the amendment, suspension, or repeal of this decision if, in the context of the Annual Joint Review of the functioning of the EU-U.S. Privacy Shield or otherwise, the Department of Commerce or other departments or agencies involved in the implementation of the Privacy Shield, or, for matters pertaining to national security, representatives of the U.S. Intelligence Community or the Ombudsperson, fail to provide information or clarifications necessary for the assessment of compliance with the Principles, the effectiveness of complaint handling procedures, or any lowering of the required level of protection as a consequence of actions by U.S. national intelligence authorities, in particular as a consequence of the collection and/or access to personal data that is not limited to what is strictly necessary and proportionate. In this respect, the Commission will take into account the extent to which the relevant information can be obtained from other sources, including through reports from self-certified U.S. companies as allowed under the USA FREEDOM Act.

(153) The Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of Directive 95/46/EC published its opinion

[209] As of the date of application of the General Data Protection Regulation, the Commission will make use of its powers to adopt, on duly justified imperative grounds of urgency, an implementing act suspending the present decision which shall apply immediately without its prior submission to the relevant comitology committee and shall remain in force for a period not exceeding six months.

on the level of protection provided by the EU-U.S. Privacy Shield,[210] which has been taken into account in the preparation of this Decision.

(154) The European Parliament adopted a resolution on transatlantic data flows.[211]

(155) [The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31(1) of Directive 95/46/EC,]

[210] Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, adopted on 13.04.2016

[211] European Parliament resolution of 26 May 2016 on transatlantic data flows ((2016/2727(RSP)).

HAS ADOPTED THIS DECISION:

Article 1

1. For the purposes of Article 25(2) of Directive 95/46/EC, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield.

2. The EU-U.S. Privacy Shield is constituted by the Principles issued by the U.S. Department of Commerce on [Date] as set out in Annex II and the official representations and commitments contained in the documents listed in Annexes I, III to VII.

3. For the purpose of paragraph 1, personal data are transferred under the EU-U.S. Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the "Privacy Shield List", maintained and made publicly available by the U.S. Department of Commerce, in accordance with Sections I and III of the Principles set out in Annex II.

Article 2

This Decision does not affect the application of the provisions of Directive 95/46/EC other than Article 25(1) that pertain to the processing of personal data within the Member States, in particular Article 4 thereof.

Article 3

Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of Directive 95/46/EC leading to the suspension or definitive ban of data flows to an organisation in the United States that is included in the Privacy Shield List in accordance with Sections I and III of the Principles set out in Annex II in order to protect individuals with regard to the processing of their personal data, the Member State concerned shall inform the Commission without delay.

Article 4

1. The Commission will continuously monitor the functioning of the EU-U.S. Privacy Shield with a view to assessing whether the United States continues to ensure an adequate level of protection of personal data transferred thereunder from the Union to organisations in the United States.

2. The Member States and the Commission shall inform each other of cases where it appears that the government bodies in the United States with the statutory power to enforce compliance with the Principles set out in Annex II fail to provide effective detection and supervision mechanisms enabling infringements of the Principles to be identified and punished in practice.

3. The Member States and the Commission shall inform each other of any indications that the interferences by U.S. public authorities responsible for national security, law enforcement or other public interests with the right of individuals to the protection of their personal data go

beyond what is strictly necessary, and/or that there is no effective legal protection against such interferences.

4. Within one year from the date of the notification of this Decision to the Member States and on a yearly basis thereafter, the Commission will evaluate the finding in Article 1(1) on the basis of all available information, including the information received as part of the Annual Joint Review referred to in Annexes I, II and VI.

5. The Commission will report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC.

6. The Commission will present draft measures in accordance with the procedure referred to in Article 31(2) of Directive 95/46/EC with a view to suspending, amending or repealing this Decision or limiting its scope, among others, where there are indications:

- that the U.S. public authorities do not comply with the representations and commitments contained in the documents annexed to this Decision, including as regards the conditions and limitations for access by U.S. public authorities for law enforcement, national security and other public interest purposes to personal data transferred under the EU-U.S. Privacy Shield;
- of a systematic failure to effectively address complaints by EU data subjects; or
- of a systematic failure by the Privacy Shield Ombudsperson to provide timely and appropriate responses to requests from EU data subjects as required by Section 4(e) of Annex III.

The Commission will also present such draft measures if the lack of cooperation of the bodies involved in ensuring the functioning of the EU-U.S. Privacy Shield in the United States prevents the Commission from determining whether the finding in Article 1(1) is affected.

Article 5

Member States shall take all the measures necessary to comply with this Decision.

Article 6

This Decision is addressed to the Member States.

Done at Brussels,

For the Commission
Vera Jourova
Member of the Commission