ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 238

Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision

Adopted on 13 April 2016

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

EXECUTIVE SUMMARY

On 29 February 2016, the European Commission published a Communication, a draft adequacy decision and the annexed texts constituting a new framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield (hereinafter: Privacy Shield), which seeks to replace the previous U.S. Safe Harbour invalidated by the Court of Justice of the European Union (hereinafter: CJEU) on 6 October 2015, in the Schrems case.

In accordance with Article 30(1)(c) of Directive 95/46/EC, the Article 29 Working Party (hereinafter: WP29) assessed these documents in order to give its opinion on the draft adequacy decision. The WP29 assessed both the commercial aspects and the possible derogations to the principles of the Privacy Shield for national security, law enforcement and public interests purposes.

The WP29 took into account the applicable EU data protection legal framework as set out in Directive 95/46/EC, as well as the fundamental rights to private life and data protection as encoded in Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental rights of the European Union. It also considered the Right to an effective remedy and to a fair trial laid down in Article 47 of the Charter, as well as the jurisprudence related to the various fundamental rights.

In addition, the analysis reflects the reasoning of the CJEU in the Schrems case regarding the Commission's margin of appreciation of an adequacy assessment. The check and controls of the adequacy requirements must be strictly performed, taking into account the fundamental rights to privacy and data protection and the number of individuals potentially affected by transfers.

The Privacy Shield needs to be viewed in the current international context, such as the emergence of big data and the growing security needs. The scope and range of collection and use of personal data has dramatically increased since the original Safe Harbour decision was issued in 2000. European data protection authorities strongly assert the importance of the principles they defend.

The WP29 first of all welcomes the significant improvements brought by the Privacy Shield compared to the Safe Harbour decision. It notes that many of the shortcomings of the Safe Harbour it had underlined in its letter of 10 April 2014 to Vice-President Reding have been addressed by the negotiators.

The fact that the principles and guarantees afforded by the Privacy Shield are set out in both the adequacy decision and in its annexes makes the information both difficult to find, and at times, inconsistent. This contributes to an overall lack of clarity regarding the new framework as well as making accessibility for data subjects, organisations, and data protection authorities more difficult. Similarly, the language used lacks clarity. The WP29 therefore urges the Commission to make this clear and understandable for both sides of the Atlantic.

With regard to the applicable law, the WP29 highlights that if the Privacy Shield adequacy decision is adopted on the basis of Directive 95/46/EC, it needs to be consistent with the EU data protection legal framework, both in scope and terminology. The WP29 considers a review must be undertaken shortly after the entry into application of the General Data Protection Regulation, in order to ensure the higher level of data protection offered by the Regulation is followed in the adequacy decision and its annexes.

On the commercial aspects of the Privacy Shield

The WP29's key objective is to make sure that an essentially equivalent level of protection afforded to individuals is maintained when personal data is processed subject to the provisions of the Privacy Shield. Although the WP29 does not expect the Privacy Shield to be a mere and exhaustive copy of the EU legal framework it considers that it should contain the substance of the fundamental principles and as a result, ensure an 'essentially equivalent' level of protection.

Notwithstanding the improvements offered by the Privacy Shield, the WP29 considers that some key data protection principles as outlined in European law are not reflected in the draft adequacy decision and the annexes, or have been inadequately substituted by alternative notions.

For instance, the data retention principle is not expressly mentioned and cannot be clearly construed from the current wording of the Data Integrity and Purpose Limitation principle. Furthermore, there is no wording on the protection that should be afforded against automated individual decisions based solely on automated processing. The application of the purpose limitation principle to the data processing is also unclear. In order to bring more clarity in the use of several important notions, the WP29 suggests that clear definitions should be agreed between the EU and the U.S and be part of a glossary of terms to be included in the Privacy Shield F.A.Q.

Because the Privacy Shield will also be used to transfer data outside the US, the WP29 insists that onward transfers from a Privacy Shield entity to third country recipients should provide the same level of protection on all aspects of the Shield (including national security) and should not lead to lower or circumvent EU data protection principles. In case an onward transfer to a third country is envisaged under the Privacy Shield, every Privacy Shield organisation should have the obligation to assess any mandatory requirements of the third country's national legislation applicable to the data importer, prior to the transfer. In general, the WP29 concludes that onward transfers of EU personal data are insufficiently framed, especially regarding their scope, the limitation of their purpose and the guarantees applying to transfers to Agents.

Finally, although the WP29 notes the additional recourses made available to individuals to exercise their rights, it is concerned that the new redress mechanism in practice may prove to be too complex, difficult to use for EU individuals and therefore ineffective. Further clarification of the various recourse procedures is therefore needed; in particular, where they

are willing, EU data protection authorities could be considered as a natural contact point for the EU individuals in the various procedures, having the option to act on their behalf.

Derogations for national security purposes

With regard to access to data by public authorities, both in the EU and in third countries, the WP29 recalls its analysis of the relevant fundamental rights contained in the Working Document on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP237).

A large step forward from the Safe Harbour decision, is that the draft adequacy decision now extensively addresses the possible access to data processed under the Privacy Shield for purposes of national security and law enforcement. The WP29 acknowledges this considerable step, as well as the increased transparency offered by the U.S. administration on the legislation applicable to intelligence data collection (Annex VI).

The WP29 however notes that the representations of the U.S. Office of the Director of National Intelligence (ODNI) do not exclude massive and indiscriminate collection of personal data originating from the EU. The WP29 recalls its long-standing position that massive and indiscriminate surveillance of individuals can never be considered as proportionate and strictly necessary in a democratic society, as is required under the protection offered by the applicable fundamental rights. Additionally, comprehensive oversight of all surveillance programmes is crucial. The WP29 takes note that there is a tendency to collect ever more data on a massive and indiscriminate scale in the light of the fight against terrorism. Given the concerns this brings for the protection of the fundamental rights to privacy and data protection, the WP29 looks to the forthcoming rulings of the CJEU in cases regarding massive and indiscriminate data collection.

Concerning redress, the WP29 welcomes the establishment of an Ombudsperson as a new redress mechanism. This may constitute a significant improvement for EU individuals' rights with regards to U.S. intelligence activities. However, the WP29 is concerned that this new institution is not sufficiently independent and is not vested with adequate powers to effectively exercise its duty and does not guarantee a satisfactory remedy in case of disagreement.

Joint review

The annual joint review mechanism mentioned in the draft adequacy decision is a key factor to the overall credibility of the Privacy Shield and the WP29 greatly welcomes the opportunity this would present to review the adequacy decision. In this regard, the WP29 understands that national representatives of the WP29 will be able to take full part in the review process but asks for clarification of the exact arrangements. The modalities (including the resulting report, its publicity and the possible consequences, as well as the financing) need to be agreed well in advance of the first review.

Conclusion

The WP29 notes the major improvements the Privacy Shield offers compared to the invalidated Safe Harbour decision. Given the concerns expressed and the clarifications asked, the WP29 urges the Commission to resolve these concerns, identify appropriate solutions and provide the requested clarifications in order to improve the draft adequacy decision and ensure the protection offered by the Privacy Shield is indeed essentially equivalent to that of the EU.

TABLE OF CONTENT

EXECUTIVE SUMMARY 2

ON THE COMMERCIAL ASPECTS OF THE PRIVACY SHIELD 3
DEROGATIONS FOR NATIONAL SECURITY PURPOSES 4
JOINT REVIEW 4
CONCLUSION 5

TABLE OF CONTENT 6

1. INTRODUCTION 9

1.1 GENERAL COMMENTS 10
1.1.1 SCOPE OF THE WP29'S ASSESSMENT 10
1.1.2 THE ASSESSMENT OF THE COMMERCIAL PART OF THE DRAFT ADEQUACY DECISION 10
1.1.3 THE ASSESSMENT OF DEROGATIONS FOR ACCESS BY PUBLIC AUTHORITIES AND THEIR SAFEGUARDS 11
1.2 THE DRAFT ADEQUACY DECISION 12
1.2.1 SCOPE OF APPLICATION OF THE EU DATA PROTECTION FRAMEWORK AND, IN PARTICULAR, OF THE DIRECTIVE 95/46/EC PRINCIPLES 12
1.2.2 LACK OF CLARITY OF THE PRIVACY SHIELD DOCUMENTS 12
1.2.3 JOINT REVIEW AND SUSPENSION 14
1.2.4 EU LEGAL FRAMEWORK UNDER REVISION 15

2. ASSESSMENT OF THE COMMERCIAL PART OF THE DRAFT ADEQUACY DECISION 15

2.1 GENERAL COMMENTS 15
2.1.1 IMPROVEMENTS 15
2.1.2 APPLICATION OF THE PRIVACY SHIELD TO ORGANISATIONS ACTING AS PROCESSOR (AGENT) 16
2.1.3 LIMITATIONS TO THE DUTY TO ADHERE TO THE PRINCIPLES 17
2.1.4 LACK OF A DATA RETENTION LIMITATION PRINCIPLE 17
2.1.5 LACK OF GUARANTEES FOR AUTOMATED DECISIONS WHICH PRODUCES LEGAL EFFECTS OR SIGNIFICANTLY AFFECTS THE INDIVIDUAL 17
2.1.6 INTERIM PERIOD FOR EXISTING COMMERCIAL RELATIONSHIPS 18
2.2 SPECIFIC COMMENTS 18
2.2.1 TRANSPARENCY 18
2.2.2 CHOICE 19
2.2.3 ONWARD TRANSFERS 20
2.2.4 DATA INTEGRITY AND PURPOSE LIMITATION 23
2.2.5 RIGHT OF ACCESS, CORRECTION AND ERASURE FOR DATA SUBJECTS 25
2.2.6 RECOURSE, ENFORCEMENT AND LIABILITY (REDRESS MECHANISMS) 26
2.2.7 PROCESSING OF HR DATA 30
2.2.8 PHARMACEUTICAL AND MEDICAL PRODUCTS 31
2.2.9 PUBLICLY AVAILABLE INFORMATION 32
2.3 CONCLUSIONS 33

3. ASSESSMENT OF THE NATIONAL SECURITY GUARANTEES OF THE DRAFT ADEQUACY DECISION 33

3.1 SAFEGUARDS AND LIMITATIONS APPLICABLE TO U.S. NATIONAL SECURITY AUTHORITIES 33

3.2 GUARANTEE A – PROCESSING SHOULD BE IN ACCORDANCE WITH THE LAW AND BASED ON CLEAR, PRECISE AND ACCESSIBLE RULES 34
3.2.1 EXECUTIVE ORDER 12333 AND PRESIDENTIAL POLICY DIRECTIVE 28 35
3.2.2 FOREIGN INTELLIGENCE SURVEILLANCE ACT 36
3.2.3 CONCLUSION 37
3.3 GUARANTEE B – NECESSITY AND PROPORTIONALITY WITH REGARD TO THE LEGITIMATE OBJECTIVES PURSUED NEED TO BE DEMONSTRATED 37
3.3.1 PRESIDENTIAL POLICY DIRECTIVE 28 37
3.3.2 FOREIGN INTELLIGENCE SURVEILLANCE ACT 38
3.3.3 CONCLUSION 40
3.4 GUARANTEE C - AN INDEPENDENT OVERSIGHT MECHANISM SHOULD EXIST 40
3.4.1 INTERNAL OVERSIGHT 40
3.4.2 EXTERNAL OVERSIGHT 41
3.4.3 CONCLUSION 42
3.5 GUARANTEE D - EFFECTIVE REMEDIES NEED TO BE AVAILABLE TO THE INDIVIDUAL 43
3.5.1 JUDICIAL REMEDIES 43
3.5.1.1 STANDING REQUIREMENT 43
3.5.1.2 PRESIDENTIAL POLICY DIRECTIVE 28 44
3.5.1.3 FOREIGN INTELLIGENCE SURVEILLANCE ACT 44
3.5.2 ADMINISTRATIVE REMEDIES 44
3.5.2.1 INSPECTORS-GENERAL 44
3.5.2.2 FREEDOM OF INFORMATION ACT 44
3.5.3 PRIVACY SHIELD OMBUDSPERSON 45
3.5.3.1 ESTABLISHMENT OF AN OMBUDSPERSON 45
3.5.3.2 THE ASSESSMENT OF THE NEW OMBUDSPERSON MECHANISM 46
3.5.3.3 CAN THE ESTABLISHMENT OF AN OMBUDSPERSON PER SE BE SUFFICIENT? 46
3.5.3.4 THE SCOPE OF APPLICATION OF THE OMBUDSPERSON MECHANISM 47
3.5.3.5 'STANDING' AND THE PROCEDURE OF THE REQUEST 48
3.5.3.6 INDEPENDENCE 49
3.5.3.7 INVESTIGATORY POWERS 50
3.5.3.8 REMEDIAL POWERS 50
3.5.4 IN CONCLUSION 51
3.6 CONCLUDING REMARKS ON SAFEGUARDS AND LIMITATIONS APPLICABLE TO U.S. NATIONAL SECURITY AUTHORITIES 51

4. ASSESSMENT OF THE LAW ENFORCEMENT GUARANTEES OF THE PRIVACY SHIELD 52

4.1 INTRODUCTION 52
4.2 APPLICATION OF THE EUROPEAN ESSENTIAL GUARANTEES TO ACCESS BY LAW ENFORCEMENT AUTHORITIES TO DATA HELD BY CORPORATIONS 53
4.2.1 ACCESS BY LAW ENFORCEMENT AUTHORITIES TO PERSONAL DATA SHOULD BE IN ACCORDANCE WITH THE LAW AND BASED ON CLEAR, PRECISE AND ACCESSIBLE RULES 53
4.2.2 NECESSITY AND PROPORTIONALITY WITH REGARD TO THE LEGITIMATE OBJECTIVES PURSUED NEED TO BE DEMONSTRATED 53
4.2.3 AN INDEPENDENT OVERSIGHT MECHANISM SHOULD EXIST 55
4.2.4 EFFECTIVE REMEDIES NEED TO BE AVAILABLE TO THE INDIVIDUAL 55
4.3 CONCLUDING REMARKS 56

5. CONCLUSIONS AND RECOMMENDATIONS 57

5.1 THREE POINTS OF CONCERN 57

1. INTRODUCTION

Following the judgment issued by the Court of Justice of the European Union (hereinafter: CJEU) on 6 October 2015 in the Schrems case[1], the Article 29 Working Party (hereinafter: WP29, the Working Party) called on the Member States of the European Union (hereinafter: the EU) and the other European institutions to open discussions with the United States (hereinafter: U.S.) authorities in order to find political, legal and technical solutions enabling data transfers to U.S. territory that respect fundamental rights.

On 2 February 2016, after more than two years of negotiations, the European Commission and the U.S. Department of Commerce (DoC) reached a political agreement on a *New framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield* (hereinafter: Privacy Shield), which seeks to replace the former U.S. Safe Harbour.

On 29 February 2016, the Commission published a Communication[2], a draft adequacy decision and the annexed texts that will constitute the Privacy Shield. In accordance with Article 30(1)(c) of Directive 95/46/EC (hereinafter: the Directive), the WP29 has assessed these documents in order to give its current opinion on the draft adequacy decision prepared by the Commission, including the underlying Privacy Shield documents. During its assessment, the WP29 has divided the work between an assessment of the commercial part of the Privacy Shield and an analysis of the safeguards put in place as regards the derogations to the principles of the Privacy Shield for national security, law enforcement and public interests purposes.

Following the judgment in Schrems, the WP29 has held several meetings with delegations from the U.S. administration, representatives of civil society organisations from both the EU and the U.S., and scholars, in order to prepare the assessment of the consequences of the Schrems judgment. During the assessment of the Privacy Shield, further meetings have been held with the European Commission and representatives of the U.S. administration. During these meetings some clarifications were provided, which have also been taken into account in this opinion. The WP29 stresses that, at this stage, these clarifications have only been informal and that they cannot be considered to form an integral part of the draft adequacy decision, since they have not yet been put in writing.

Nevertheless, the WP29 especially welcomes the commitment given by the DoC during these meetings to co-operate with the data protection authorities of the EU member states regarding the application of the Privacy Shield and to provide for instructions and legal interpretation regarding the application of the Privacy Shield to be published on their websites.

[1] Case C-362/14 - Maximilian Schrems v. Data Protection Commissioner, 6 October 2015 (hereinafter: Schrems)
[2] COM(2016)117 final, 29 February 2016

1.1 General comments

1.1.1 Scope of the WP29's assessment

The WP29 first of all took into account the applicable data protection framework in the Member States of the European Union, including Article 8 of the European Convention on Human Rights (hereinafter: ECHR) protecting the right to private and family life as well as Articles 7, 8 and 47 of the Charter of Fundamental rights of the European Union (hereinafter: the Charter) respectively protecting the right to private and family life, the right to protection of personal data and the right to an effective remedy and fair trial. It also took into consideration the relevant jurisprudence, as well as the requirements of the Directive.

The requirement for a third country to ensure an adequate level of data protection was further defined by the CJEU in Schrems. The Court did not only explain that the provisions of the Directive must be interpreted "in the light of the fundamental rights guaranteed by the Charter"[3] and in particular Articles 7 and 8. It also indicated that the wording 'adequate level of protection' must be understood as "requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the Directive read in the light of the Charter"[4]. For the former Safe Harbour decision, such an assessment has never been made with a sufficient level of detail. The WP29 therefore assessed the draft adequacy decision in light of the requirement to provide an analysis of the level of protection of fundamental rights and freedoms being *essentially equivalent* to that guaranteed within the EU. The WP29 stresses this opinion contains its principal concerns, but that given the limited time that has passed since the draft adequacy decision was published further issues may be discovered at a later date.

The WP29 acknowledges that by defining the word 'adequate' in Article 25(6) of the Directive as 'essentially equivalent', the CJEU further detailed adequacy in the Schrems case. The Court has underlined that the term 'adequate level of protection', although not requiring the third country to ensure a level of protection identical to that guaranteed in the EU legal order, must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is *essentially equivalent* to that guaranteed within the European Union by virtue of the Directive read in the light of the Charter.

1.1.2 The assessment of the commercial part of the draft adequacy decision

The WP29 has already explained the way it applied the core EU data protection principles to transfers of personal data to third countries in its Working Document 12 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive'[5]. The WP29 tried to find the equivalent safeguards which ensure a level of

[3] Schrems, §38
[4] Schrems, §73
[5] Adopted by the WP29 on 24 July 1998, see in particular page 6

protection equivalent to the principles guaranteed in the Directive, notably regarding purpose limitation, data quality and proportionality, transparency, security, rights of access, rectification and opposition, data retention and restrictions on onward transfers. A similar method has been used in the opinions issued by the WP29 at the time of the assessment of the original Safe Harbour adequacy decision[6] as well as in recommendations made by the Working Party in its letter to former Vice-President and EU Commissioner for Justice Viviane Reding, published on 10 April 2014[7].

1.1.3 The assessment of derogations for access by public authorities and their safeguards

The assessment of the derogations for access by public authorities to personal data covered by the Privacy Shield is a complex one, especially taken into account the increased awareness of the data protection authorities and the general public of U.S. surveillance programmes following the Snowden revelations. The Working Party recognises and welcomes the U.S. administration's effort to increase transparency on surveillance programmes and their willingness to include additional safeguards in the Privacy Shield. At the same time, the WP29 stresses that any interference with the fundamental rights to private life and data protection need to be justifiable in a democratic society. The CJEU criticised the fact that the Safe Harbour decision did not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference. Nor does it refer to the existence of effective legal protection against interference of that kind.[8]

The WP29 has therefore analysed the current U.S. legal framework and practices of U.S. intelligence agencies as they are described in the Annexes to the Draft Decision, as well as the conditions under which they allow any interference with the fundamental rights to respect for private life and to data protection as protected under the European legal framework.

In order to evaluate if any interference would be justifiable in a democratic society, the assessment was conducted in light of the European jurisprudence on fundamental rights which sets four essential guarantees[9] for intelligence activities:

A. Processing should be in accordance with the law and based on clear, precise and accessible rules: this means that anyone who is reasonably informed should be able to foresee what might happen with her/his data where they are transferred;
B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated: a balance needs to be found between the objective for which the data are collected and accessed and the rights of the individual;
C. An independent oversight mechanism should exist, that is both effective and impartial: this can either be a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks;

[6] See WP62, WP32, WP27, WP23, WP21, WP19, WP15 and WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf
[8] Schrems, §§87, 88
[9] The European Essential Guarantees are based on the jurisprudence of the CJEU and the ECtHR and are set out in more detail in the WP29 Working Document WP237, published on 13 April 2016.

D. Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body.

1.2 The draft adequacy decision

The WP29 first of all welcomes the fact that a new adequacy procedure can be launched less than six months after the CJEU declared the Safe Harbour decision invalid. Given the amount of data transfers that take place between the EU and the U.S. on a daily basis, which the WP29 recognises is a vital part of the economy on both sides of the Atlantic, legal clarity is needed sooner rather than later.

The WP29 however regrets that the draft adequacy decision published by the Commission does not include a comprehensive assessment of the domestic law and the international commitments of the U.S. in the form of an adequacy report, as has been the regular practice in the past in similar procedures and in line with Article 25 of the Directive. This has prevented the WP29 from carrying out a complete analysis of the legal context in which the Privacy Shield will operate. It notes for example that the current draft adequacy decision does not include findings on the privacy and data protection legislation that exists in the U.S., both at the Federal and at State level, including sectorial legislation, nor on legislation allowing for non-surveillance related forms of public access. Also the relation between data transfers under the Privacy Shield and under other existing adequacy findings like the EU-U.S. Passenger Name Records (PNR) Agreement and the Terrorist Finance Tracking Program (TFTP) Agreement is not defined.

1.2.1 Scope of application of the EU data protection framework and, in particular, of the Directive 95/46/EC principles

The WP29 recalls that under the EU data protection legal framework, and in particular under the Directive (Article 4(1)), Member States laws apply not only to the processing operations carried out by data controllers established on their territory, but also where data controllers (although not established in the EU), make use of equipment situated on EU territory, in particular for the collection of personal data. As a consequence, EU Member State law applies to any processing that takes place prior to the transfer to the U.S., either in the context of activities of an organisation established in the EU or through the use of equipment situated in the EU used by an organisation not established in the EU. The WP29 requests that this is made explicit in the draft adequacy decision.

It should be clear that the Privacy Shield Principles will apply from the moment the data transfer takes place. Moreover, the WP29 recalls that data controllers established in the EU and transferring data to a data processor in the U.S. remain subject to EU data protection law.

1.2.2 Lack of clarity of the Privacy Shield documents

The fact that the principles and guarantees afforded by the Privacy Shield are set out in both the adequacy decision and in its annexes makes the information both difficult to find, and at times, inconsistent. This contributes to an overall lack of clarity regarding the new framework

as well as making accessibility for data subjects, organisations, and data protection authorities more difficult. Similarly, the language used lacks clarity. The WP29 therefore urges the Commission to make this clear and understandable for both sides of the Atlantic.

The WP29 suggests to include a separate annex providing defined core terms which are applied in the Privacy Shield documents. A common and unambiguous understanding of the obligations imposed by the Privacy Shield adequacy decision is crucial for its effective functioning on both sides of the Atlantic, and as such the WP29 is concerned that due to the numerous cross-references and non-aligned formulations as well as the complexity of the framework documents, difficulties will be had regarding the consistency, intelligibility and clarity of the implementation of the Privacy Shield.

More importantly, the Privacy Shield documents make use of terminology that is not consistent with the vocabulary generally used in the EU when dealing with data protection. This is not necessarily a problem, as long as it is clear what the corresponding terminology under EU law (and under U.S. law) would be. The WP29 regrets to note however this is not the case, including in the draft adequacy decision. For example, the word 'access' is used in chapter 3 of the draft adequacy decision in a sense that implies the collection of personal data, instead of allowing someone to see data that is already collected. Access by companies to the data and the individuals' right of access are two separate notions that should not be confused.

The WP29 stresses that the terminology should also be used consistently throughout the documents, including in the draft adequacy decision. This is currently not the case, for example for the notions of 'processing' and 'personal data'. Both are in principle well-defined in Annex II, but not consistently applied throughout the documents, which results in loopholes in the protection.[10,11]

The WP29 welcomes that definitions of some of the terms used have been included in the documents constituting the Privacy Shield. However, this is not the case for a number of other essential terms, including 'Agent' or 'processor', 'key-coded data', 'anonymised data' and 'EU individual', which in the view of the WP29 warrant a clear definition on which both the U.S. and the EU agree, in order to avoid confusion at a later stage for both the data controllers

[10] Some of the clauses solely enumerate some sorts of data processing operations instead of making use of the term 'processing'. This results in loopholes in the protection. E.g., according to the wording of Annex II, III.6.f, the Privacy Shield Principles would be applicable only where the organisation "stores, uses or discloses" the received data (i.e. not for other operations covered by the term 'processing', such as collecting, recording, alteration, retrieval, consulting, erasure.). Data security would be imposed only for "creating, maintaining, using or disseminating" personal information (Annex II, II.4). The definition of personal data is also limited to data 'received' and 'recorded'. As a further example the Notice Principle (Annex II, II.1.a.iv) states that the certified organisation must inform individuals about the purposes for which it "collects and uses" data about them. Annex II, III.9.a.11 solely mentions data which are 'transferred' or 'accessed'. Even if it appears that in most of such cases the intention is not to limit the scope of the Principles or to create protection gaps, this inconsistent terminology entails the risk of entailing such gaps. As the term 'processing' is defined in the Principles, it is crucial to make use of it in a consistent manner. in order to avoid the now existing loopholes. Otherwise too much room for presumably unintended interpretation would exist, which could otherwise lead to misinterpretation of the wording of the decision.

[11] The definition of 'personal data' included in Annex II, I.8.a, refers to "data about an identified or identifiable individual". Supplemental Principle however states that in relation to human resources data, the Principles only apply when "identified records are transferred or accessed". The WP29 considers that this opens up a possibility to process personal data in a way that is not compliant with the data protection principles under EU law, nor with the general definition of personal data under the Privacy Shield.

and processors using the Privacy Shield, the supervisory authorities and the general public. An easy solution would be to add a glossary of terms to the Privacy Shield F.A.Q.

The WP29 also points to the legitimate grounds for processing of sensitive data in Supplemental Principle 1 (Annex II, III.1), in cases where an organisation does not have to obtain explicit consent (opt-in). This Supplemental Principle 1 can be understood as detailing the legitimate grounds for the collection of data in the EU as this list is similar to Article 8 of the Directive. The WP29 would like to recall that any processing (including collection and transfer) of sensitive data subject to EU law has to be made on legitimate grounds according to article 8 of the Directive. The Privacy Shield cannot be interpreted as offering alternative grounds for such processing. For instance, in the view of the WP29 it is not possible for a U.S. organisation to collect data subject to EU law on the basis of U.S. employment law (see Annex II, III.1.a.v). The WP29 therefore stresses that any interpretation of Supplemental Principle 1 may only lead to its application to sensitive data already transferred after having been collected in the EU on legitimate grounds listed in article 8 of the Directive.

The WP29 finally notes a lack of clarity as to the question who can be considered to be an EU individual and thus benefits from protection under the Privacy Shield: all EU citizens or all persons residing in the EU. This is of particular importance in relation to the right to the redress, including the access to the Ombudsperson mechanism. Additionally, the adequacy decision should address the question to what extent the Privacy Shield will also apply to citizens / residents of the countries of the EEA and Switzerland, which in the past did enjoy coverage by the Safe Harbour scheme.

1.2.3 Joint Review and suspension

The WP29 welcomes the fact that the European Commission and the U.S. administration have agreed to regularly review the practical application of the Privacy Shield. This joint review is a known practice in the EU data protection community for a number of years, especially in relation to the agreements on the exchange of PNR data with third countries and the TFTP Agreement. The WP29 furthermore welcomes the fact that an unspecified number of representatives from data protection authorities can take part in these joint reviews.

Given its experience with joint reviews in recent years, the WP29 would like to make clear that it expects the joint review of the Privacy Shield to be more extensive than the PNR and TFTP joint reviews. In particular, it is desirable that the joint review will not only include meetings with representatives of U.S. agencies, organisations and businesses, but also on-the-spot verifications of certain elements of the Privacy Shield. The DPA representatives in the joint review should be able to make suggestions for such on-the-spot verifications.

The WP29 considers that a joint review requires a joint assessment of the findings. Thus far, the results of joint reviews have been presented in a Commission staff document, for which the approval of non-Commission joint review team members was not required. For the Privacy Shield joint review, the WP29 would appreciate if the findings report could indeed be

a shared product. Alternatively, the release of a separate DPA joint review report could be considered.

Finally as regards the joint review, the WP29 recalls the promise of the Commission that costs incurred by the representatives of the WP29 during joint reviews shall be reimbursed by the Commission. The Working Party assumes this will also apply for the Privacy Shield joint review, in any case for a reasonable number of DPA representatives.

The WP29 recommends that at the latest three months before the first Privacy Shield joint review should take place, the modalities for the joint review are agreed between the Commission, the U.S. administration and the WP29 and put down in writing.

1.2.4 EU legal framework under revision

The Privacy Shield adequacy decision is the first adequacy decision that has been drafted following the principled agreement on the text of the General Data Protection Regulation. The WP29 has however ascertained that the Privacy Shield does not yet reflect the future situation. For example, important new notions like the right to data portability and additional obligations on data controllers, including the need to carry out data protection impact assessments and to comply with the principles of privacy by design and privacy by default, have not been included in the Privacy Shield. The WP29 would therefore like to suggest that the Privacy Shield, as with any existing adequacy decisions, is reviewed shortly after the GDPR enters into application. An explicit reference to this review process in the final adequacy decision would be appreciated.

2. ASSESSMENT OF THE COMMERCIAL PART OF THE DRAFT ADEQUACY DECISION

2.1 General comments

2.1.1 Improvements

The WP29 welcomes the improvements brought by the Privacy Shield and the will of its negotiators to try and address the Safe Harbour shortcomings it had underlined. In particular, compared to the Safe Harbour, improvements can be noted on the following elements: the insertion of some key definitions such as ‘personal data’, ‘processing’ and ‘controller’, the mechanisms set up to ensure the oversight of the Privacy Shield list and the now mandatory external or internal reviews of compliance. Improvements are also made to the Access principle and the WP29 notes that correction and deletion rights are now provided when data is used in a way incompatible with the Privacy Shield Principles. In addition, it is now made clear that the individual must receive both confirmation that data are being processed regarding him and communication of the data processed.

The WP29 also welcomes the reinforcement of the legal guarantees where onward transfers are taking place and the commitments of the DoC and the Federal Trade Commission (FTC) to enforce the obligations set out by the Privacy Shield.

2.1.2 Application of the Privacy Shield to organisations acting as Processor (Agent)

The extent to which the Privacy Shield Principles are applicable to certified organisations receiving personal data from the EU for mere processing purposes (referred to as 'Agents' or 'processors') unfortunately remains unclear. While the provisions under Annex II, III.10.a. do mention data transfers to certified organisations for such purposes - i.e. mentioning the requirement to enter into a contract - they lack any indication as to how the Privacy Shield Principles shall apply to processors (Agents). This causes uncertainty both for the certified U.S. organisations receiving data for processing purposes and for EU companies carrying out data transfers to certified organisations acting as data processors, as well as for the individuals whose data are processed. In consequence, it will be difficult to determine which duties actually apply to Shield organisations processing personal data received from the EU in their role as processors. Clarification is therefore certainly required.

It has to be taken into consideration that several of the obligations included in the Principles are not suitable for data processors, as it is always the data controller that determines the purposes and means of the processing of the data (cf. the definition of 'Controller' under Annex II, I.8.c). It is for this reason that some obligations contained in the Principles, if applied to an organisation acting as Agent, may contradict the data processing contract required under EU law (the contract mentioned under Annex II, III.10.a.). For example, the data processing contract will generally not authorise the data processor (Agent) to onward transfer data to a third party controller, even under the circumstances mentioned in Annex II, II.3.a. Onward transfers to third party Agents should only be authorised following the prior approval of the data controller. Additionally, according to the requirements of EU law, a processor (Agent) will not be able to provide individuals with full Notice as intended by the Notice principle (Annex II, II.1), for example because this organisation does not determine the purposes of the processing.

It is therefore crucial to clarify in the Principles that in case of such contradiction, the provisions of the data processing contract and particularly the instructions of the organisation transferring the data out of the EU will prevail. Without such clarification, the Principles could be interpreted and applied in a manner that offers too much control capacities to the Shield Agent and this would put the EU data exporter at risk of violating his obligations as a data controller under EU data protection law to which it is subject when transferring data to a Shield organisation acting as an Agent. In addition, this lack of clarity gives the impression that the processor might reuse the data as he wishes.

Furthermore, specific rules should be provided for when an organisation acts as a data processor (Agent), in order to ensure that this organisation respects the data controller's instructions. It should be made clear that U.S. organisations receiving data for mere processing purposes cannot decide to process the data on their own behalf. In the absence of specific rules applicable to organisations acting as processor, it is difficult to determine against which rules the processor (Agents) would be able to self-certify.

2.1.3 Limitations to the duty to adhere to the Principles

Annex II, I.5. provides, among others, for exemptions from the Principles when data covered by the Privacy Shield is used for reasons of national security[12], public interest, law enforcement, or following statute, government regulation or case law which creates conflicting obligations or explicit authorisations. Without full knowledge of U.S. law at both the Federal and at state level, it is difficult for the WP29 to assess the scope of this exemption and to consider whether those limitations are justifiable in a democratic society. It would be essential that the European Commission also includes in its draft adequacy decision an analysis of the level of protection where those exemptions would apply. The WP29 calls on the Commission to ensure that the EU is informed of any statute or government regulation that would affect adherence to the principles, either currently applicable or at the time when new statutes or regulations enter into force in the U.S.

2.1.4 Lack of a data retention limitation principle

The Data Retention Limitation principle (Article 6(1)e of the Directive) is a fundamental principle in EU data protection law imposing that personal data must only be kept as long as necessary to achieve the purpose for which the data have been collected or for which they are further processed.

However, the WP29 cannot find in the documents constituting the Privacy Shield any reference to the necessity for data controllers to ensure that the data are deleted once the purpose for which they were collected or further processed has become obsolete. Hence, as it seems, the Principles do not impose to the certified organisations a limit for the period of retention of the data comparable to what is imposed by the data retention limitation principle under EU law.

The wording of the Data Integrity and Purpose Limitation principle (Annex II, II.5) can in no way be considered as creating an obligation for an organisation acting as a controller to delete data after it is no longer necessary for the purposes for which the data have been collected or further processed or for an organisation acting as a processor to delete data after the termination of the service agreement.

The Working Party underlines that the lack of provisions imposing a limit on the retention of data under the Privacy Shield gives organisations the possibility to keep data as long as they wish, even after leaving the Privacy Shield, which is not in line with the essential data retention limitation principle.

2.1.5 Lack of guarantees for automated decisions which produces legal effects or significantly affects the individual

The Privacy Shield does not provide any legal guarantees where individuals are subject to a decision which produces legal effects concerning or significantly affecting them and which is

[12] See chapter 3 for more comment on the use of personal data covered by the Privacy Shield for national security purposes and chapter 4 for law enforcement purposes.

based solely on automated processing of data intended to evaluate certain personal aspects relating to them, such as their performance at work, creditworthiness, reliability, conduct, etc.

The necessity to provide for legal guarantees for automated decisions (producing legal effects or significantly affecting the individual**)** in order to provide an adequate level of protection has already been underlined by the WP29 in its Working Document 12.

This necessity becomes even more crucial since ever developing new technologies enable more companies to consider the implementation of automated decision making systems which may lead to weakening the position of individuals left without any recourse against those computer made decisions. Where decisions made solely by those automated systems impact upon the legal situation of individuals or significantly affecting them (for example, by black listing and thereby depriving individuals of their rights) it is crucial to provide sufficient safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis..

2.1.6 Interim period for existing commercial relationships

The Privacy Shield foresees that the Principles apply immediately upon certification. However, organisations that will certify within the two first months following the Privacy Shield's framework effective date of entry into force, will have to bring any existing commercial relationships with third parties into conformity with the Accountability for Onward Transfer Principle as soon as possible. In any event they should do so no later than nine months from the date upon which they certify to the Privacy Shield.

This means that existing contracts to the extent necessary need to be brought in line with the Principles between two and nine months after certification. During this interim period, Notice and Choice suffices. The WP29 insists on the fact that transfers can take place on the basis of the Privacy Shield only from the moment that the organisation can fully comply with all the Shield requirements. A possibility to send data during an interim period without the recipient being in a position to fully comply with the Shield principles cannot be considered to meet the conditions for a legal transfer and is therefore not acceptable.

2.2 Specific comments

2.2.1 Transparency

a) General remarks on Notice

The WP29 welcomes the more comprehensive and detailed requirements set forth under the Notice Principle, in particular that the Notice will have to include a link to or a web address of the Privacy Shield List and refer to the access right of individuals as well as the alternative dispute resolution mechanisms.[13] However, the WP29 suggests to be more explicit on the

[13] Annex II, II.1; the WP29 also refers to the second Commission recommendation made in the Communication COM(2103)847 as well as the WP 29 letter to Vice-President Reding of 10 April 2041, in particular point 4 under 'Transparency'.

other rights (to correct, delete where inaccurate or processed in violation of the Principles) covered.

The documents constituting the Privacy Shield do raise concern regarding the time when a Privacy Shield organisation needs to provide Notice to an individual. Annex II, II.1.b states that "notice must be provided (…) when individuals are first asked to provide personal information to the organisation or as soon thereafter as is practicable, but in any event before the organisation uses such information for a purpose other than that for which it was originally collected or processed by the transferring organisation or discloses it for the first time to a third party". The WP29 considers that in many situations, a U.S. Shield organisation will not directly collect data from the data subject and so the timing of the notice should be at the point the data is recorded by the Shield organisation.

The WP29 notes that the actual implementation of the requirements with regard to the Notice Principle and the privacy policy should be assessed at the first annual review of the Privacy Shield.

b) Public availability of the privacy policy

The WP29 welcomes the fact that it is now explicit that the DoC will check if companies that have public websites have published their privacy policy on this website or, where they have no public websites, where the privacy policy is made available to the public.[14]

c) Publication of privacy conditions of contracts with processors

The Privacy Shield provides, amongst the conditions under which Privacy Shield organisations can transfer data to a processor (Agent), for an obligation for self-certified organisations to "provide a summary or a representative copy of the relevant privacy provisions of its contract with that Agent to the Department upon request" (see Annex II, II. 3.b.v). The Working Party welcomes this transparency requirement towards the DoC.

2.2.2 Choice

The Privacy Shield provides for a right to opt-out to disclosure of personal information to a third party or to the use of personal information for a purpose materially different[15] (Annex II, III, 2). In addition, individuals benefit from an 'opt-out' right to the use of personal information for direct marketing purpose at any time (Annex II, III.12.a)[16].

Except for the context of direct marketing purposes, no detail is provided about the manner and the moment this opt-out may be exercised. The WP29 considers that the simple reference to the existence of this right in the privacy policy cannot be sufficient but an *individualised*

[14] See the first recommendation made by the European Commission in its Communication COM(2013)847 and the WP29 letter to Vice-President Reding, 10 April 2014, in particular point 3 under 'Transparency'

[15] The Supplemental Principle 14.c.I provides for the right to withdraw from a Clinical trial, which might be seen as the right to object or to withdraw consent.

[16] This is identical as what was provided in the Safe Harbour scheme (F.A.Q. 12) and not changed has been made as this regard.

opportunity to exercise this right should be offered *before* the disclosure or re-use of personal information.

Moreover, the WP29 emphasises that a general right to object (on compelling grounds relating to the data subject's particular situation), being understood as a right to ask to terminate the processing about one's data whenever the individual has compelling legitimate grounds relating to his particular situation, should be offered within the Privacy Shield[17]. The WP29 strongly recommends that the draft adequacy decision makes clear that the right to object should exist at any given moment, and that this objection is not limited to the use of the data for direct marketing[18].

The WP29 fears that the lack of definition of what is to be regarded as a 'materially different' purpose will lead to confusion and legal uncertainty. It should be clarified that in any case, the Choice principle cannot be used to circumvent the Purpose limitation principle[19]. Choice should be applicable only where the purpose is materially different but still compatible since the processing for incompatible purpose is prohibited (Annex II, II.5.a). It has to be clarified that the right to opt-out cannot enable the organisation to use data for incompatible purposes. Hence, it recommends harmonising the related wording by using a single and defined wording (e.g. "materially different but nevertheless compatible purpose").

Clarification would be helpful as to where a decision taken to process data for another purpose or to disclose information falls under EU law. In this situation the usual EU legal conditions regarding this processing (such as the prohibition on processing for incompatible purposes, to provide for a legitimate ground for the processing and the need to inform the individual) will directly apply including to the U.S. organisation falling under the scope of EU law. In practice, this means that it will be for the EU exporter taking such a decision to ensure transparency and lawfulness of the processing according to EU law. Therefore, the choice principle will apply only where the decision is taken exclusively by the U.S. Shield organisation not submitted to EU law.

2.2.3 Onward transfers

a) Scope

The WP29 is concerned with the situation where onward transfers of personal data take place from a Privacy Shield certified organisation in the U.S. to a recipient in a third country.

The Shield should not only be seen as a tool to transfer EU data from the EU to the U.S. but will also serve as a tool to be used to transfer data from the U.S. to third countries. Provisions on onward transfers are therefore an important element of the Shield that should provide sufficient guarantees and an adequate level of protection when data are onward transferred outside the U.S. One particular issue is linked to national security and law enforcement.

---

[18] See WP29 letter to Vice-President Reding, under 'Choice'.
[19] A concrete example of further incompatible processing authorised under the Choice principle is provided under Supplemental principle 9.b.i (see the WP29 comment about it under the point related to 'HR data'.

The Accountability for Onward Transfers principle of the Privacy Shield is not limited to recipient data controllers, processors or Agents established in the U.S. Therefore, onward transfers to a third country could take place on the basis of the Privacy Shield, even if the third country has laws providing for public access to personal data, for example for purposes of surveillance. This puts EU data at risk of unjustified interferences with the fundamental rights protection.

In any case of an onward transfer to a third country, every Privacy Shield organisation should be obliged to assess the mandatory requirements of the third country's national legislation applicable to the data importer prior to the transfer. If a risk of substantial adverse effect on the guarantees, obligations and level of protection provided by the Privacy Shield is identified, the U.S. Privacy Shield organisation acting as a Processor (Agent) shall promptly notify the EU data controller before carrying out any onward transfer. In these cases the data exporter is entitled to suspend the transfer of data and/or terminate the contract. Where there is such a risk of substantial adverse effect, a Shield organisation acting as a controller should not be allowed to onward transfer the data, as this would compromise its duty to provide the same level of protection as under the Principles in case of onward transfers (see Annex II, II.3.a).

Similarly, in the event of a change in the third country's legislation which is likely to have a substantial adverse effect on the guarantees, obligations and level of protection provided by the Privacy Shield, the U.S. Privacy Shield organisation acting as a Processor (Agent) should be obliged – by the Privacy Shield – promptly to notify this change to the data exporter as soon as it becomes aware of it, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract. Accordingly, in such a case, a Shield organisation acting as a controller should not be allowed to onward transfer as it has a duty to provide the same level of protection as under the Principles (see Annex II, II.3.a).

The WP29 recalls its position that if the EU data controller is aware of an onward transfer to a third party outside the U.S. even before the transfer to the U.S. takes place, or if the EU data controller is jointly responsible for the decision to allow onward transfers, the transfer should be considered as a direct transfer from the EU to the third country outside the U.S. This means Articles 25 and 26 of the Directive are applicable to the transfer instead of the Privacy Shield onward transfer principle.

b) Transfers from a Privacy Shield organisation to a third party controller

The WP29 welcomes the duty to put in place contracts (Annex II, II.3.a) to ensure that a third party Controller will provide at least the same level of privacy protection as is required by the Privacy Shield principles. The purpose is to ensure that personal data continue to be protected adequately, even after having been transferred onward. However the WP29 has some remarks on the proposed conditions.

<u>Lack of reference to the Purpose Limitation principle</u>

The WP29 recommends also inserting a clear reference to the Purpose Limitation principle (Annex II, II.5) within the conditions for onward transfers to a third party controller (Annex II, II.3.a). This would make clear that onward transfers may not take place where the third party controller will process data for an incompatible purpose.

Exemption to the need of contract for intra-group transfers between controllers

An exemption to the need of contract is provided for intra-group transfers between controllers. In such a scenario, the Principles state that the continuity of the protection could be offered by Binding Corporate Rules (BCRs) or "other intra-group instruments (e.g. compliance and control programmes)" (Annex II, III.10.b). The WP29 considers that the reference to 'other intra-group instruments' does not guarantee legally binding commitments made by the other members of the group. Since the WP29 and the EU legislation[20] generally favour binding commitments to frame intra-group transfers, it is important to avoid that the Privacy Shield will be used in a way to circumvent this requirement. The WP29 recalls that, in any case, onward transfers from the U.S. to third countries planned even before the transfer to the U.S. takes place, or that are subject to joint controllership with the EU data controller[21], have to be considered as a direct transfer from the EU to the third country outside the U.S. Articles 25 and 26 of the Directive are therefore applicable to the transfer.

c) Transfers from a Privacy Shield organisation to a third party processor (Agent)

The WP29 welcomes the fact that a contract for onward transfers is now mandatory for receiving entities acting as processors (Agents) regardless of their participation to the Privacy Shield or if they benefit from another adequacy finding solution. The WP29 also welcomes the additional safeguards framing these onward transfers (Annex II, II.3.a.i; II.3.a.iii; II.3.a.iv; II.3.a.v; II.7.d). The last point (Annex II, II.7.d) concerns the obligation to remain liable when data are disclosed to an Agent. However, it seems that this guarantee will not apply in case an organisation has chosen to cooperate with a DPA (see Annex II, III.5.a in fine). The WP29 does not understand the reason for such an exemption and considers that liability should apply even in this case.

Lack of reference to the purpose limitation principle

The WP29 notes that the Accountability for Onward Transfer principle (Annex II, II.3) explains that personal data may be transferred to a third party acting as an Agent only for limited and specified purposes, but does not explicitly say that these limited and specified purposes have to be compatible with the initial purposes for which the data were collected as well as with the instructions of the controller. More clarity is needed on this point. The WP29 therefore suggests to ensure the adequacy decision provides more detail, for example by inserting a clear reference to the Purpose Limitation principle (Annex II, II.5), according to

[20] The need of binding and enforceable commitments is also underlined in the GDPR whatever the tool used (BCRs, contractual clauses, codes of conduct or certification).
[21] For instance, for HR data.

which data may not be processed (including disclosed) for incompatible purposes within the onward transfer principle (in addition to the opt-out principle).

Need for more additional obligations for Privacy Shield organisations acting as processor (Agent) onward data to another processor (Agent)

The absence of clear rules where the Shield organisation is acting as an Agent (i.e. on behalf an EU controller) imply a loophole and might prevent the EU controller to remain into control. A Shield organisation receiving the data as an Agent of an EU controller has to respect the EU controller's instructions. This should be expressly stated in the Principles in order to ensure that the non-respect of those instructions will not only lead to a breach of the contract (Annex II, III.10.a.ii) but also to a violation of the Privacy Shield principles.

The possibility for a Shield organisation acting as an Agent to subsequently transfer data to a third party Agent has to be made transparent to the Controller and be subject to its prior approval. It should therefore be clearly stated that it is the contract signed by the Agent with the EU controller (referred to in F.A.Q. 10 as the 'Article 17 contract') that determines whether an onward transfer is allowed.[22]

The current conditions applicable to the onward transfer to an Agent are built on the assumption that the Shield organisation acts as a controller and can therefore decide by itself on the possible intervention of a third party Agent. This should however not be possible where the Shield organisation acts as an Agent. Otherwise, the EU controller will be deprived from its control capacities.

The relevant privacy provisions of the contract concluded with the third party Agent must be made available to the controller and must also to provide at least the same level of protection as provided by the contract signed with the controller.

2.2.4 Data Integrity and Purpose Limitation

a) Proportionality

On a minor point, the WP29 refers to its letter to Vice-President Reding in which it wrote that "a processing of personal data could, even under a strict respect of Notice and Choice, be not proportionate with regards to the interests' rights and freedoms of the data subject or society. The principle of proportionality or reasonableness is to be respected at all stages of the processing and should be applicable in addition to the principles of Notice and Choice"[23].

The Privacy Shield (Annex II, II.5.a) states that the information must be limited to what is relevant for the processing. The WP29 would prefer if this wording is amended in the final adequacy decision, since the mere fact that the data shall be relevant to the processing is not sufficient to make the processing proportionate. In order to meet the proportionality principle, the processing should be limited to the data that are necessary for the processing at stake.

[22] See WP29 letter to Vice-President Reding, 10 April 2014, point 4 under Onward Transfer
[23] See WP29 letter to Vice-President Reding, 10 April 2014, p.8

b) Accuracy

The Data Integrity and Purpose Limitation principle (Annex II, II.5) also states: "To the extent necessary for those purposes, an organisation must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current". The WP29 notes that this is exactly the same wording as used in the Safe Harbour arrangement. The WP29 doubts that the wording "to the extent necessary to these purposes" should be included, since the accuracy of the data in its view should not depend on the purpose of the processing. The WP29 would prefer if this connection is not made in the final adequacy decision.

c) Purpose limitation

Where personal data are transferred to a U.S. organisation by a data controller established in the EU, the data exporter should explicitly inform the U.S. organisation of the purposes for which the data had been originally collected. This is essential to determine whether a change of purpose occurs after the transfer, thus triggering the Notice and Choice principles, and would contribute to allocating risk and liability.

The Data Integrity and Purpose Limitation principle (Annex II, II.5) states that an organisation may not process personal information in a way incompatible with the purposes for which it has been collected or subsequently authorised by the individual. The Choice principle (Annex II, II.2) however provides for an opt-in for the 'use' of sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual, as well as data regarding criminal records) for purposes which are materially different from the purposes for which the data have originally been collected or subsequently authorised by the individual. This opt-in is not required in the situations mentioned in Supplemental Principle 1.a (Annex II, III.1.a). As regards non-sensitive personal information, an opt-out regime is provided for.

The WP29 notes that the scope of the Purpose Limitation principle is different under the Notice, the Choice and the Data Integrity and Purpose Limitation principles. In fact, the terms 'incompatible purpose' and 'materially different purpose' are used within the same text without a clear definition of both these concepts[24].

The WP29 has serious concerns about the fact that such inconsistency might lead to great difficulties to reconcile the Data Integrity and Purpose Limitation principle (Annex II, II.5) with the Choice principle (Annex II, II.2), since one states that the data cannot be processed in a way that is incompatible with the purposes for which they were collected, while the other provides for an opt-out mechanism in case the data are processed for a purpose that is materially different from the original purpose.

[24] The WP29 noted that some other expressions are also used: "a use that is not consistent with" (Annex II, III.14.b.ii), a "use for different purposes" (Annex II, III. 9.B.i), a "use for a purpose other than that for which it was originally collected" (Annex II, II.1.b). This unclarity might lead to the absence of sufficient guarantees as regard the purpose limitation principle.

Thus the Choice principle, can be read as authorizing a further incompatible processing[25]. According to the WP29, it has to be made explicit that an organisation shall not be authorised to process data for a purpose materially different where this purpose is incompatible according to the Purpose Limitation Principle. In other words, it should be clear that the Choice principle is not an exemption to the Purpose Limitation.

In any case also, if the further processing can be considered as being compatible, then Notice and Choice principles should also apply.

2.2.5 Journalistic exceptions

The journalistic exceptions to the processing of personal data are covered in Supplemental Principle 2 (Annex II, III.2). It is understood that these provisions reflect the U.S. constitutional protection of free speech. Therefore, the Privacy Shield documents state that "personal information found in previously published material disseminated from media archives is not subject to the requirements of the Privacy Shield Principles" (Annex II, III.2.b). This exemption seems to include any further processing by any data controller or processor, i.e. not to be limited to further processing for journalistic purposes. As already stated in the letter to Vice-President Reding of 10 April 2014, the WP29 would have preferred to see a more limited approach to journalistic exceptions, more in line with the principle as applied in the EU, as well as the right to delisting following the Google Spain case[26].

2.2.5 Right of access, correction and erasure for data subjects

According to the Privacy Shield individuals have the right to obtain *confirmation* of whether their data are processed by the organisation and to have *communicated to them* such data (Annex II, III.8.a.i). However, the obligation for organisations to answer requests from individuals concerning the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data is disclosed is quite weak. The WP29 considers the details to be provided to the data subject should be mentioned in the body of the text, instead of in a footnote only and have to be drafted as a clear obligation (linked to Annex II, III.8.a.i.1).

According to Supplemental Principle 8 "access needs to be provided only to the extent that an organisation stores the personal information" (Annex II, III.8.d.ii). This rule should not be interpreted restrictively, in the sense that access has to be provided, in principle, to data processed in any way by an organisation, and not only stored. Therefore, for the purposes of the effectiveness of the right of access, it is important to make clear that 'stores' means 'processes' in the meaning of the definition provided for in Annex II, I.8.b. The application of this rule should be attentively examined during the joint review of the Privacy Shield.

[25] See also the comment under the Choice principle. The WP29 considers that the fact that the Onward transfer rules (Annex II, II.3) only refers to the Choice principle and not to the Purpose Limitation principle, increases the risk of such an understanding.
[26] Case C-131/12 – Google Spain v. Agencia Española de Protección de Datos and Mario Costeja González, 13 May 2014.

Concerns remain with regard to the list of exceptions provided under Annex II, III.8.e.(i), which is similar to the one provided by F.A.Q. 8 of the Safe Harbour and which has a tendency to incline the balance towards the interests of the organisations. In this sense, access to their own personal data will not be granted to individuals, for the following reasons: "breaching a professional privilege or obligation" (Annex II, III.8.e.3), "prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organisations" (Annex II, III.8.e.4), and "prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization" (Annex II, III.8.e.5). These reasons should be read in addition to the general exemption on confidential commercial information included in Annex II, III.8.c. Therefore, an individual will never have access to his or her data in the situations enumerated above, no balance of rights and interests between those of the individual and those of the organisation being stroke to reach a solution to the access request.

The WP29 recalls that the right to access their own data is granted to individuals in Article 8(2) Charter. While this is not an absolute right, it is fundamental for the right to the protection of personal data because it facilitates the exercise of the other rights of the data subject, such as correction and erasure.

As regards the rights to correction and erasure, The WP29 welcomes a significant improvement brought by the Privacy Shield Principles, compared to the Safe Harbour Principles, providing that those rights are granted not only in the situations where data is inaccurate, but also where data has been processed in violation of the Principles (Annex II, II.6).

2.2.6 Recourse, enforcement and liability (redress mechanisms)

a) Effective exercise of EU individuals' rights of redress

The WP29 acknowledges the commitments of U.S. authorities as regards the different layers of the redress mechanism. However, considering the complexity and the lack of clarity of the overall architecture of the mechanism, the WP29 fears that, in practice, the effective exercise of the data subject's right might be undermined. The WP29 points out that the quality of redress mechanism should prevail over the quantity of mechanisms available to the EU individuals. There are also concerns that most, if not all, of the recourse mechanisms foresee a procedure in the U.S., thus complicating monitoring of the procedure by the EU DPAs.

In fact, the recourse mechanism provided for in the Privacy Shield concentrates first on the possibility for the data subject to "vindicate their rights and pursue case of non-compliance with the Privacy Principles through direct contacts with the U.S. self certified company"[27]. Moreover, organisations must designate an independent dispute resolution body to investigate and resolve individual complaints. The WP29 welcomes the fact that this will be organised at no cost to the individual.

[27] European Commission, draft adequacy decision, §30

Alternatively, complaints could be directly made with the Federal Trade Commission, even if there is no duty for the FTC to deal with them. A DPA could also refer a complaint and the DoC has committed to review and undertake best efforts to facilitate resolution of complaints (Annex I) which will be given 'priority consideration' by the Federal Trade Commission (Annex II, III.7.e). However, the prioritisation of complaints by the FTC does not give any certainty to the data subject that its complaints will be dealt with.

As a last resort, individuals will have the possibility to invoke binding arbitration. The arbitration panel will be based in the U.S. and will be subject to review by U.S. Courts.

The Privacy Shield also offers the possibility for the organisation to choose cooperation with EU DPAs (Annex II, III.5.a). This is even mandatory for human resources data collected in the context of an employment relationship (Annex II, III.9.d.ii). In such a scenario, alternative dispute resolution (ADR) will not be applicable (Annex II, III.5.a). The Privacy Shield does not clearly establish how the cooperation with EU DPAs will be organised in practice. In particular, it is unclear whether the panel will deal with all cases or if each different case will be dealt with by a different panel.

The WP29 considers that more detail is required in the adequacy decision where the competence of DPAs to deal with complaints is concerned. This apparently depends on the qualification of the organisation, but it is unclear in what way.

Where the organisation is acting as an Agent on behalf of an EU controller, individuals will in any case have the possibility to complain to the competent EU DPA. The situation will be similar for both human resources and other commercial data processing.

Where the Privacy Shield organisation is acting as a data controller, the competence of a DPA to deal with the complaint will be restricted to processing subject to EU law (processing under responsibility of EU controller – including joint controllership with US organisation – or where the Privacy Shield organisation would be directly subject to EU law, for example by using of equipment in EU). However, for data processing carried out only under U.S. law, the Privacy Shield mechanisms will apply exclusively. In order to overcome language barriers and lack of knowledge of the U.S. legal system, it could be helpful if EU DPAs are entitled to act as an intermediary for the individual's complaint or to assist him/her in ADR proceedings with U.S. organisations or during their contacts with the U.S. authorities if the DPA considers this appropriate.

The WP29 stresses that the mechanism explained in the Privacy Shield does not follow the earlier recommendation according to which EU individuals should be "able to bring claims for damages in the European Union" as well as be "granted the right to lodge a claim before a competent EU national court."[28] It would be welcomed if Privacy Shield organisations were to include such a possibility in their privacy policies.

[28] See WP29 letter to Vice-President Reding, 10 April 2014

In order to ensure effectiveness, the WP29 recommends that the system should preferably allow for EU DPAs to represent the data subject and act on his behalf or to act as an intermediary. Alternatively, it should contain specific jurisdiction clauses entitling data subjects to exercise their rights in Europe.

b) Arbitration

Final arbitration procedures are not yet finalised, which complicates the assessment by the WP29. As it seems that the arbitration scheme will take place under U.S. law and that the only language of procedure will be English, EU DPAs may want to be entitled to assist individuals in the process.

Furthermore, the arbitration procedure has been put in place due to the fact that there was no insurance that a complaint will be dealt with as the FTC does not have a duty to deal with every complaint. Should an EU individual feel the need to be assisted by an attorney, the WP29 notes he/she will have to cover his/her own attorney's fees, which may prevent individuals to submit their complaint to the arbitration procedure.

c) Oversight, enforcement and effectiveness of redress mechanisms

<u>Conditions to get into the Shield</u>

According to the CJEU "the reliability of a system of self-certification […] is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights […]."[29]

The WP29 notes that the Privacy Shield role of the DoC in the certification process appears to be reduced to a mere checking of completeness of documents. Although the WP29 acknowledges that self-certification does not imply a systematic a priori check of the implementation of the privacy policies, the DoC should at the very least commit to systematically check that privacy policies include all Privacy Shield principles. Such commitment is mentioned in the draft adequacy decision but cannot not be clearly identified in the representation letter of the DoC.[30]

A violation of the Privacy Shield principles might go unnoticed for a long period of time and might only be detected after serious harm has been caused to the data subject's fundamental rights, possibly beyond repair. Hence, this approach might contravene the European precautionary principle.

<u>Transparency by means of the Privacy Shield list and record of organisations removed from the list</u>

Considerable improvements have been made with regard to transparency towards the data subject. In addition to all U.S organisations that have self-certified to the DoC, the new

[29] CJEU, Schrems, §81
[30] European Commission, draft adequacy decision, §34

Privacy Shield List will also contain a record of all organisations removed from the Privacy Shield List, including the reason why an organisation was removed.[31] The Privacy Shield website of the DoC will further focus more on the target audiences in a way that it will facilitate the verification of the type of information covered by an organisation's self-certification as well as the privacy policy that applies to the covered information and the method the organisation uses to verify its adherence to the principles.[32] The WP29 welcomes the fact that it is now explicit that the DoC will check if companies that have public websites publish their privacy policy on this website or, when they do not they have a public website, where the privacy policy is made available to the public.[33] The documents are more informative about the content of the privacy policy, too.[34]

The WP29 considers a problem could arise if an organisation which is already included in the Privacy Shield List subsequently extends its certification to other categories of data. In such cases, the list will not reflect the different periods of applicability of the Principles to the different categories of data. This creates the risk that EU individuals and businesses cannot fully assess if a specific data set is indeed subjected to the Privacy Shield Principles, and if so, since when. To avoid this deficiency, the Working Party recommends that an organisations' record in Privacy Shield List shall separately specify for each category of personal data the data of entry into application of the self-certification.

The WP29 welcomes the fact that the DoC will maintain a record of organisations that have been removed from the Privacy Shield List and that this record will include an explanation clarifying that those organisations are no longer assured of the benefits of the Privacy Shield, but must continue to apply the Principles to personal data received while being a Privacy Shield certified organisation, as long as they retain such data (Annex I, p. 3). However, since some organisations that have been removed from the Privacy Shield List may choose to return or delete the data received under the Privacy Shield, while other organisations will retain data that they have received under the Shield, it is important to provide more transparency on this issue to individuals. Therefore, the record of companies maintained by the DoC should specify whether the organisation still retains personal data received under the Privacy Shield, or whether it has returned or deleted such data. If the organisation still retains such data, the record should explicitly state that the organisation must continue to apply the Principles to such data.

Furthermore, the record maintained by the DoC should, mention that these organisations are no longer assured of the benefits of the Privacy Shield for new transfers, meaning that the organisation is no longer permitted to receive personal data from the EU under the Principles.

[31] Annex I, p. 5 and Annex II, II.1; the WP29 also refers to the fourth Commission recommendation in Communication COM(2103)847 as well as the WP29 letter to Vice-President Reding, 10 April 2014, in particular point 5 under 'Transparency'.
[32] Annex I, p. 8; the WP29 also refers to its letter to Vice-President Reding, 10 April 2014, in particular point 2 under 'Transparency'.
[33] Annex I, p. 3 and 4; the WP29 also refers to the first Commission recommendation in Communication COM(2103)847 as well as the WP29 letter to Vice-President Reding, 10 April 2014, in particular point 3 under 'Transparency'.
[34] Annex I, p. 5 and 6 and Annex II, III.6

Verification procedures

To verify that the self-certification is effective in practice, organisations can make self-assessment or outside compliance reviews. The WP29 regrets that employees' training is only required when an organisation opts for verification through self-assessments (Annex II, III.7.c). It also seems that the need to check that policies are accurate, comprehensive, prominently displayed, implemented and accessible is only required if the organisation opts for internal review (self-assessments) and that review by an outside mechanism is only limited to compliance with the privacy policy of the organisation.

A posteriori

The WP29 welcomes that the FTC and the DoC are invested with investigatory powers in cases of complaints. Moreover, the WP29 notes that DoC will have the possibility to make ex officio verifications, in particular through sending questionnaires. However, the WP29 would like to make sure that such an approach is sufficient to meet the CJEU's requirement of effective detection and supervision mechanisms of infringement. In fact, the WP29 still has questions remaining the exact power of U.S. enforcement authorities to conduct on-site inspections on the premises of self-certified organisations to investigate Privacy Shield violations, on how *exequatur* of an EU authority decision could be obtained on the U.S. territory and on whether the sanctions under the Privacy Shield are deterrent in practice.

2.2.7 Processing of HR data

Scope

Supplemental Principle 9 (Annex II, III.9) applies to personal information about an employee (past or present) collected in the context of the employment relationship. According to the wording of Supplemental Principle 9.a.ii, the Privacy Shield Principles solely apply when "identified records are transferred or accessed". This term of 'identified record' is not in line with the definition of 'personal data' under Annex II, I.8.a., which comprises "data about an identified or identifiable individual" and therefore does not align with the definition used in the Directive[35].

Supplemental Principle 9.a.ii states that "Statistical reporting relying on aggregate employment data and containing no personal data or the use of anonymised data does not raise privacy concerns". This statement contradicts a number of Opinions issued by the WP29. The WP29 would like to emphasise that aggregated data can still be re-identified and therefore should be regarded as personal data[36].

[35] As already underlined, the limitation to records that are 'transferred or accessed' is also not in line with the term 'processing' (Annex II, I.8.b).
[36] See Opinion 4/2007 on the concept of personal data as well as Opinion 05/2014 on Anonymisation Techniques

Notice, choice and purpose limitation

Supplemental Principle 9.b.i, provides an example of application of the Notice and Choice Principles, where HR data is used for a different purpose. The example relates to a U.S. organisation which "intends to use personal information collected through the employment relationship for non-employment related purposes, such as marketing communications". In this scenario, the change of purpose is authorised under the condition to respect the Notice and Choice principle. According to the WP29, the further processing of human resources data for direct marketing purposes will in most cases have to be considered as an incompatible purpose and therefore contrary to the purpose limitation principle (Annex II, II.5.a). In addition, the WP29 considers that the Choice cannot be an appropriate basis for the employee to 'consent' (opt-out) to a change of purpose, in the employment context where such consent might not be entirely free.

The WP29 has strong doubts that the main focus of the Privacy Shield to the Choice principle as a condition to further use data for another purpose meet the OECD Privacy Guidelines as there is no sufficient guarantees to prevent that this opt out mechanism could also be used for further processing for incompatible processing. Supplemental Principle 9.b.iv provides for a broad and explicit exemption to the Notice and Choice principles "to the extent and for the period necessary to avoid prejudicing the ability of the organisation in making promotions, appointments or other similar employment decisions". First, the use of HR data for such purposes should already be explicitly stated at the collection of the data. Moreover, the wording "other similar employment decisions" is too vague and too broad. It will have as consequence that HR data will be totally exempted from the notice and choice principle where processed in the context of the employment relationship. The term is so broad, it does not allow assessing whether the further use is compatible with the original purpose. The WP29 recommends the deletion of this exception.

Right to Access

Supplemental Principle 9.e.i also provides for an exemption to apply the Access Principle or from entering into a contract with a third party controller for HR data where it relates to occasional employment-related operational, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees and provided that Notice and Choice are complied with. The WP29 does not see any reasonable justification for such an exemption and recommends to delete this paragraph.

2.2.8 Pharmaceutical and medical products

Scope

The Privacy Shield considers that transfers of key-coded data from the European Union to the U.S. in the context of Pharmaceutical and Medical products do not constitute transfers that would be subject to the Privacy Shield (Annex II, III.14.g.i). However, the transfer of key-coded data enjoys protection under European data protection law. This means that in practice

the Privacy Shield cannot cover such transfers. The WP29 calls on the EU Commission to explicitly provide that the draft adequacy decision will not cover the transfer of key-coded data for pharmaceutical or medical reasons and as a consequence, such transfers must be covered by other safeguards, such as Standard Contractual Clauses (hereinafter: SCCs) or BCRs. The WP29 suggests this could be clarified in the final adequacy decision.

Transfers for Regulatory and supervision purposes (Annex II, III.14.d)

The WP29 is concerned that under these provisions personal data which is due to the medical context mostly of sensitive nature may be transferred to regulators in the U.S. Since the Privacy Shield is designed for data transfers between private entities it appears that a public body like a U.S. regulator is not eligible to self-certify under the Privacy Shield which raises the question of adequate data protection for such transfers. If such transfers need to be administered for regulatory purposes, appropriate measures must be taken to ensure continuous protection of EU data subject's fundamental rights. The WP29 underlines the fact that the draft adequacy decision does not provide any findings on this point. Therefore, the WP29 does not have any guarantee that the sensitive data of EU-data subjects will enjoy adequate protection in this context.

Additionally, the WP29 notes it does not understand why the purpose of 'marketing' is listed as an example of processing for future scientific research. Also the reason to place onward transfers to company locations and other researchers (Annex II, III.14.d) under the heading "Transfers for Regulatory and Supervision Purposes" is unclear. These issues require clarification in the final adequacy decision.

Product Safety, Efficacy monitoring (including reporting to government agencies) and tracking of patients using certain medicines or medical devices

The Privacy Shield provides for an exemption to the Notice, Choice, Onward transfer and Access principles to the extent that adherence to the Principle interferes with compliance with regulatory requirements. The Draft Adequacy decision does not provide for any findings as regards the situation where Privacy Principles interferes with compliance with regulatory requirements. If the WP29 might understand that governments investigations may justify limits to Notice and the right of Access to protect investigations, the WP29 does not see the reasons that can justify such broad exemptions where processing are taking place by the organisation or by a third party in the private sector. For instance, as the treatments of patients are more and more individualised, such a broad exemption of the Privacy principles in case of tracking of patients using certain medicines or medical devices is unacceptable as this type of care will become common. This also applies where data are used by pharmaceutical companies for Product Safety, Efficacy monitoring (test or sale of new medicines).

2.2.9 Publicly available information

The exception to the right of access in the case of publicly available information and public record information (Annex II, III.15.d and e) raises concerns to the extent that an individual,

when exercising his/her right of access, is interested to know whether a particular controller processes data about himself/herself, and also to know what data is being processed, in order to be able to control the processing of his/her data. The WP29 has repeatedly stated that according to EU law data subjects always have the right to access their data, and, where necessary, to require rectification or erasure of the data if the data have not been processed lawfully or if they are incomplete or inaccurate, regardless of whether or not the personal data have been published.[37] If the individual's request for access is rejected on the grounds that the data were obtained from publicly available sources or public records, the individual would lose the ability to control the accuracy of the data and to control whether the data were lawfully made public in the first place.

The Privacy Shield however exempts public records and publicly available information from the principles of Notice, Choice, Access, and Accountability for Onward Transfers (Annex II, II.15.b). These exemptions seem too broad in comparison with the Directive and raise concerns, as they impair, among others, the individuals' possibilities to control the accuracy of their data and to restrict dissemination of their data.

2.3 Conclusions

The WP29 recognises that the U.S. authorities and the European Commission have brought significant improvements to the commercial aspects for data transfer between the two continents. Taking into account the above analysis, the WP29 however finds that the commercial part of the Privacy Shield requires further clarification on many points. For example, the lack of an explicit data retention principle, is cause for concern. Therefore, the WP29 has serious concerns that the Privacy Shield can ensure a level of protection that is essentially equivalent to that in the EU.

The adequacy decision needs to further clarify the Purpose Limitation and Choice principles. There remains the risk of loopholes regarding several principles, notably the onward transfers, the complaint handling mechanism and the processing of HR or Pharmaceutical data. Additionally, how the Privacy Shield Principles are to be applied to data processors (Agents) requires further elaboration and special attention is needed to ensure a clear and unambiguous application of terminology.

3. Assessment of the national security guarantees of the Draft Adequacy Decision

3.1 Safeguards and limitations applicable to U.S. national security authorities

Interferences with the fundamental rights to private life and data protection may be allowable, provided that such an interference is justifiable in a democratic society. This means that the Privacy Principles are not absolute and that derogations may be possible, but only if the applicable (essential) guarantees are met. Consistent with the goal of enhancing privacy protection, organisations should moreover strive to implement the Principles fully and

[37] See WP20, p. 4

transparently, including indicating in their privacy policies where exceptions to the Principles permitted by the U.S. legal framework will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organisations are expected to opt for the higher protection where possible.

In Annex II, I.5 it is stated that, "adherence to the Privacy Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts.

The question is whether the derogations mentioned in Annex II. are justifiable in a democratic society. According to the draft adequacy decision of the Privacy Shield, the Commission found 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 Privacy Shield to what is strictly necessary to achieve the legitimate objective in question."[38]

Using the framework as set out in Section 1.2 of this Opinion and with the representations of the U.S. authorities and the findings of the Commission in mind, the WP29 has assessed the current U.S. legal framework and practices of U.S. intelligence agencies and the conditions under which they allow any interference with the fundamental rights to respect for private life and data protection as protected under the European legal framework. This assessment is based on the analysis of the Presidential Policy Directive 28 (PPD-28), Executive Order 12333 (EO12333) and on the various legal bases established by the Foreign Intelligence Act (FISA - Section 104, Section 402, Section 215, Section 501 and Section 702). The WP29 has relied on Annex VI of the Privacy Shield which consists of a letter prepared by the Office of the Director of National Intelligence (ODNI) regarding safeguards and limitations applicable to U.S. national security authorities and summarising the information which has been provided to the European Commission regarding the U.S. signals intelligence collection activities.

3.2 Guarantee A – Processing should be in accordance with the law and based on clear, precise and accessible rules

According to European law, an interference has to be in accordance with laws, established policies and procedures and sufficiently clear and accessible (within the margin of discretion awarded to individual countries), to give citizens an adequate indication as to the

[38] Draft Commission Decision pursuant to Directive 95/46/EC of the European parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, §75

circumstances in which, and the conditions under which, public authorities are empowered to resort to surveillance measures.[39]

The WP29 notes that signals intelligence activities are conducted on the basis of an accessible legal framework. All laws mentioned in Annex VI (PPD-28, FISA, USA FREEDOM ACT, FOIA) are online available for the general public (in and outside of the U.S.). Annex VI provides a summary of the governing legal framework, the collection limitations, the retention and dissemination limitations, compliance and oversight, transparency and redress. The U.S. legal system for intelligence activities consists of a number of different documents including individual agencies reports, policies and procedures that need to be analysed to gain a better understanding of how activities are conducted, both in theory and in practice. In that regard, the WP29 has concentrated on a limited number of points that it considers crucial.

3.2.1 Executive Order 12333 and Presidential Policy Directive 28

The scope of EO12333 is wide; in principle, all foreign intelligence data collection can take place at the discretion of the U.S. President based on the Order. However it has been argued that since the introduction of FISA, EO12333 can only be used for the collection of data outside the U.S. territory. The WP29 notes that EO12333 does not provide a lot of detail regarding its geographical scope, the extent to which data can be collected, retained or further disseminated, nor on the nature of offences that may give rise to surveillance or the kind of information that may be collected or used.

In the understanding of the WP29, the main purpose of the Presidential Policy Directive 28 (PPD-28) is to prescribe the limits for the collection and the processing of personal data, no matter which surveillance programme is used and where data was obtained.

PPD-28 is a directive of the President of the United States laying down consistency principles with which signals intelligence collection shall be authorised and conducted but PPD-28 is not a legal basis for collection. PPD-28 is effective by imposing those principles on intelligence community bodies to implement it in their policies and procedures. The directive applies to signals intelligence activities, regardless of the location of the data at the time when it is collected, inside or outside the U.S. It therefore also applies to the data collected for signals intelligence purposes when they are transferred from the EU to the U.S.

In particular, PPD-28 states that the signals intelligence activities shall be as tailored as feasible[40]. Regarding the use of the data, it lays down procedures of data minimisation

[39] ECtHR Zakharov §247 "The Court has previously found that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance (see Kennedy, cited above, § 159). At the same time, the Court has also emphasised that in matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."

(including conditions for the retention and dissemination of the data), data security and access by relevant staff [i.e. rules containing safeguards limiting the risks of abuse and improper use], data quality and oversight. These guarantees apply regardless of the nationality of the data subjects, i.e. to U.S. and non-U.S. persons.

During the transmission of the data to the U.S., the safeguards established by PPD-28 are also applicable. Annex VI contains a commitment of the ODNI that if the U.S. Intelligence Community were to collect data from transatlantic cables while it is being transmitted to the United States, "it would do so subject to the limitations and safeguards set out herein, including the requirements of PPD-28"[41]. WP29 notes that there continues to be a lack of established jurisprudence determining the legality of cables interception if it were to be carried out by any country. In any case, the U.S. neither confirms nor deny that they do use cables interception as a means for intelligence data collection.

The concept of 'signals intelligence' is not defined in PPD-28 nor in any other applicable text.

3.2.2 Foreign Intelligence Surveillance Act

Overall, the text of FISA appears to be clearer and more precise. However, the interpretation of many provisions in the light of PPD-28 and thus their practical application largely depends on the implementation made by the various agencies. While a full report on the implementation of the new safeguards is not yet available, U.S. delegates have informed representatives of the WP29 that the implementation of the PPD-28 safeguards has indeed been completed and is carried out in a similar way across the U.S. intelligence community.

More precisely, Section 501 is relatively clear on the kind of intelligence operations that can be mandated: "the production of any tangible things (including books, records, papers, documents, and other items)". However, it should be noted that the fact that the definition of 'tangible things' includes 'other items' makes the scope of this authority quite broad.

Section 702, which allows for data to be collected from non-U.S. persons reasonably believed to be outside the United States in order to obtain foreign intelligence information,[42] does not provide the same level of detail as Section 501. Concerning its scope, Section 702 targets electronic communications service providers established in the U.S. for the collection of foreign intelligence information of individuals located outside the U.S. The definition of 'foreign intelligence information' is broad. It includes amongst others, "information with respect to a foreign power or foreign territory that relates to the conduct of foreign affairs of the United States"[43] which raises some uncertainty as to the type of information that can be collected in practice.

---

[40] "Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritised." (Section 1(d))

[41] Privacy Shield Annex VI, Office of the Director of National Intelligence (ODNI) letter regarding safeguards and limitations applicable to U.S. national security authorities, p. 2

[42] 50 U.S. Code §1881a (D)(1)

[43] 50 U.S. Code § 1801 (e) (2).

Despite the declassification of documents, reports to Congress and the oversight reports of the Privacy and Civil Liberties Oversight Board (hereinafter: PCLOB), the application of the FISA, including the scope and the use of the specified selection terms, remains unclear and confusing. The use of specified selection terms ('tasked selectors') is referred to in a PCLOB report[44], but it is the understanding of the WP29 that this does not correspond to the targeting rules following section 702[45]. They are not referenced in generally accessible rules, as far as the WP29 has been able to confirm.

3.2.3 Conclusion

Overall, the WP29 notes that the applicable texts relating to intelligence activities are available online and that the U.S. authorities have been taking a number of important steps towards for transparency.

The WP29 recognises that since 2013 a great number of documents such as policies, procedures, FISC decisions and other declassified documents has been published. Moreover, the PCLOB has released important reports on the activities conducted on the basis of section 702, and the USA FREEDOM Act. A similar report is expected on activities under EO12333.

Several legislative annexes that could shed light on the implications of the Executive Order on individuals outside the United States and any applicable safeguards are classified, and as such not accessible to the public or individuals possibly affected by their application. Where texts have been declassified, they only provide limited value and insight regarding intelligence activities.

Despite the effort made to explain the workings of EO12333 following the Snowden revelations, in particular through the adoption of PPD-28, the current practical application of EO12333 remains unclear. The WP29 notes that Annex VI of the Privacy Shield does not provide detailed information on the functioning of EO12333.

Whilst the WP29 welcomes the limitations overlain by PPD-28, it is difficult to consider whether the U.S. legal framework for surveillance is sufficiently foreseeable, i.e. contains "adequate indication[s] as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures" as further clarification including the publication of the PCLOB report into EO12333 is awaited.

3.3 Guarantee B – Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

3.3.1 Presidential Policy Directive 28

PPD-28 introduced limitations regarding the purposes for which personal data can be used and on the conditions under which they can be disseminated and impacts the collection of signals intelligence, no matter which legal basis is used.

[44] PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA, p. 32
[45] 50 U.S. Code § 1881a(D)

In particular, Section 1 of PPD-28 provides that U.S. signals intelligence activities must always be 'as tailored as feasible'. While recognising this limitation, it is difficult to determine whether 'as tailored as feasible' means that all data collection is necessary and proportionate.

PPD-28 recognises that bulk collection continues to be permitted "in order to identify new or emerging threats and other vital national security information that is often hidden within the large and complex system of modern global communications".[46] The WP29 notes that PPD-28 states that "signals intelligence collected in 'bulk' means the authorised collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)".

PPD-28 imposes limits on the use of signals intelligence collected in bulk as regards the purpose of the use. These six purposes for which data can be collected in 'bulk', including counter-terrorism and other forms of serious (transnational) crimes. The WP29's analysis suggests that the purpose limitation is rather wide (and possibly too wide) to be considered as targeted.

PPD-28 has not removed the possibility for the indiscriminate collection of personal data in bulk and that the scale of such collection possibilities remains unclear and potentially broad. In this regard, the WP29 notes that in Annex VI, the ODNI affirms that "any bulk collection activities regarding internet communication that the U.S. Intelligence Community performs through signals intelligence operate on a small portion of the Internet[47] and therefore would appreciate further evidence being provided through transparency measures.

3.3.2 Foreign Intelligence Surveillance Act

The Section 215 and Section 702 FISA minimisation procedures were introduced in order to protect U.S. persons from far reaching government access to their data. These limitations do not officially apply to foreigners, even though U.S. government officials have stated repeatedly in both public and private meetings with WP29 representatives that the scope of application of the minimisation procedures has since in practice been extended to cover all persons, no matter their nationality or habitual place of residence.

Section 702 specifies that an acquisition authorised "shall be conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States limiting data collection to what is considered as compliant with the reasonable search principle. In this regard, no difference is made between U.S. and non U.S. companies". In other words, under the condition that the Fourth Amendment applied to all data collected in the U.S., 'bulk' collection taking place in the U.S. would be 'unreasonable' and thus unconstitutional.

[46] PPD-28, Section 2 and Privacy Shield Annex VI, Office of the Director of National Intelligence (ODNI) letter regarding safeguards and limitations applicable to U.S. national security authorities, p. 3

[47] Privacy Shield Annex VI, Office of the Director of National Intelligence (ODNI) letter regarding safeguards and limitations applicable to U.S. national security authorities, p. 4; the WP29 recalls in this regard the report of the findings by the EU Co-Chairs of the ad hoc EU-US Working Group on Data Protection, which states that "Communications data make up a very small part of global internet traffic", given that the "vast majority of global internet traffic consists of high-volume streaming and downloads such as television series, films and sports" (§3.1.2 of the report)44

The WP29 welcomes the findings in the PCLOB report that "in practice, 'non-U.S. persons' also benefit from the access and retention restrictions required by the different agencies' minimisation and/or targeting procedures due to the cost and difficulty of identifying and removing U.S person information for a large body of data means that typically the entire data set is handled in compliance with the higher U.S data standards".

The WP29 further notes that according to the PCLOB findings, "the programme does not operate by collecting communications in bulk". The 2014 Statistical Transparency Report issued by the ODNI confirms this finding. Additionally, according to PCLOB report, "tasked selectors", such as an e-mail address or a telephone number, are used to target the surveillance.[48]

The corresponding available public rules relating to targeting do however not provide for such targeted rules and only aim to avoid the targeting of U.S. persons or U.S.-based persons. Moreover, the benefits that according to the PCLOB apply to non-U.S. persons in practice are not legally binding or statutorily established, since the available legislation relating to targeting do not provide for such targeted rules and only aims to avoid targeting U.S. persons or U.S.-based persons.

The WP29 furthermore recalls that for Section 702 purposes, persons are not only individuals, but also groups, entities, associations, corporations, or foreign powers. Moreover, the fact that collection is justified by "a significant purpose of the acquisition is to obtain foreign intelligence information" leaves some uncertainty regarding its purpose and necessity. However, WP29 welcomes the information provided in Annex VI that the total number of individuals targeted under Section 702 in 2014 were approximately 90.000 individuals[49]. The first review of the Privacy Shield will provide an opportunity for further evidence of the targeting rules to be demonstrated.

So far, there is no conclusive jurisprudence on the legality of massive and indiscriminate data collection and subsequent use of personal data for the purpose of combating crime, including the question under what circumstances such collection and use of personal data could take place. The CJEU is expected to address this question at least to some extent in the course of 2016, both in the joined cases Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Davis and others[50] and in the advice to be given on the validity of the PNR Canada agreement.[51] In the meantime the WP29 recalls that it has consistently considered that massive and indiscriminate collection of data in any case cannot be regarded as proportionate.[52]

[48] PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA, p. 32
[49] Annex VI, p. 11
[50] CJEU, Joined Cases C-203/15 and C-698/15
[51] CJEU, Case A-1/15
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

3.3.3 Conclusion

Despite the limitations brought following the introduction of PPD-28, the concerns of the WP29, particularly regarding the proportionality of the data collection, remain. First of all, there are indications that the U.S. continue to collect massive and indiscriminate data, or at least do not exclude that they may still do so in the future. The WP29 has consistently held that such data collection is not in conformity with EU law and is therefore not acceptable.

Secondly, the WP29 notes that also targeted data processing, or processing that is 'as tailored as feasible', can still be considered to be massive. Whether or not such massive data collection should be allowed or not is currently subject to proceedings before the CJEU. For this reason, the WP29 shall not make a final assessment as to the legality of targeted, but massive data processing. However, it stresses that if targeted, but massive data processing would be allowed, the targeting principles should apply to both the collection and the subsequent use of the data, and cannot be limited to just the use. In any case, a clarification of the draft adequacy decision is needed in relation to the six purposes mentioned in PPD-28 for which data can be collected 'in bulk'. The WP29 is, at this stage, not convinced these purposes are sufficiently restricted to ensure the data collection is indeed restricted to what is necessary and proportional.

3.4 Guarantee C - An independent oversight mechanism should exist

The U.S. does not have one single oversight body at the federal level tasked to oversee the implications of intelligence and surveillance programmes for privacy and data protection. Rather, the U.S. intelligence activities are subject to a multi-layered oversight process: a distinction can be made between internal and external oversight. The WP29 recognises that the U.S. oversight bodies reporting practice is very detailed and mostly public.

3.4.1 Internal oversight

All intelligence and security agencies have staff members that are responsible for ensuring compliance with their legislative framework including Inspectors-General whose primary task is to assess overall compliance of the work of the agencies with the legislation, including but not limited to the laws related to privacy and data protection. The Inspectors-General are established by statute and are (or soon will be) all appointed by the President followed by Senate confirmation, in an attempt to ensure that they will be organisationally independent and report to Congress. The WP29 considers the Inspectors-General therefore 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. For the time being, some concerns remain regarding Inspectors-General that are still appointed by the Director of the agency they oversee.

The Inspectors-General can make recommendations which can then be referred to the Department of Justice and to the PCLOB or even to the Congressional committee who can enforce the recommendations. If a violation is found by the Inspector-General, it can be dealt

with through internal and policy measures and reported to the Congress. The Inspector-General has the authority for instance to carry out both audits and inspections.

The WP29 notes that the reports of the Inspector-General can be withheld from the public and that an Inspector-General can also be prevented from reporting if the information inspected is classified. However, the reports will at all times to subject to Congressional oversight, which is an essential safeguard, even if it does not provide grounds for individual recourse.

All agencies have Privacy and Civil Liberty Officers who assist with the compulsory self-reporting system with Congressional oversight.

Overall, the internal oversight mechanisms in place can be considered as fairly robust; however, in order to justify an interference with the fundamental rights to privacy and data protection, oversight needs to be fully independent. And while the WP29 respects and appreciates the work of the various privacy and civil liberty officers, it cannot conclude that they meet the required level of independence to act as independent supervisor.

3.4.2 External oversight

External oversight consists of a number of different mechanisms: judicial oversight under Section 501 and 702 ensured by the FISA Court (hereinafter: FISC), the oversight of the Congress's Select Intelligence Committees and the tasks performed by the PCLOB.

The WP29 recalls that ideally, as has also been stated by the CJEU and the ECtHR, the oversight should be in the hands of a judge in order to guarantee the independence and impartiality of the procedure. Until recently, the FISC procedure was an ex parte procedure, without the possibility of the individuals concerned to be heard, or even to be aware of the case. Also today, the FISC procedure remains ex parte, but following the adoption of the USA FREEDOM Act the amici curiae to the FISC were introduced. The amici curiae act independently, but are not established to defend specific individuals that may be involved in the case.

The USA Freedom Act created a group of amici curiae to brief the FISC on important cases. The Court has selected five lawyers who have obtained the appropriate security clearances and provide technical advice, attend FISC hearings and supply briefs, and argue on the merits of a case from a privacy and civil rights perspective. However, they will only do so in important cases or when new legal questions arise.[53]

Section 215 is almost fully subject to ex ante (but not ex post) judicial oversight since all programmes using Section 215 as a basis for collection are subject to approval from the FISC. The PCLOB report specifies that "Section 702 differs from this traditional FISA electronic surveillance framework both in the standards applied and in the lack of individualised determinations by the FISC. Under the statute, the Attorney General and Director of National

[53] Freedom Act TITLE IV--FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS Sec. 401. Appointment of amici curiae

Intelligence make annual certifications authorizing the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information, without specifying to the FISC the particular non-U.S. persons who will be targeted. […] There also is no requirement that the government demonstrate probable cause to believe that a Section 702 target is a foreign power or Agent of a foreign power, as is required under traditional FISA."[54]

Within Congress, the Select Intelligence Committees also have an oversight task approving intelligence activities, in particular through the vote of the budget. Senate and House Intelligence Committees receive classified briefings about intelligence activities. The AG must report to these committees every six months about FISA electronic surveillance. It remains unclear to the WP29 to what extent they are able to discuss the processing of personal data of individual persons, especially of non-U.S. persons.

The PCLOB is an independent part of the executive branch in the U.S. government which is vested with two fundamental authorities; (1) to review and analyse actions the executive branch takes to protect the [U.S] nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties, and (2) to ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the nation from terrorism. The WP29 notes that the PCLOB has subpoena power and access to classified information. While performing its task, it also checks the efficacy of the programmes. Its oversight is not performed prior to, but after the fact. PCLOB has demonstrated its independent powers by disagreeing with the President of the United States on legal issues. In particular, it found that Section 215 telephone metadata programme was not legally authorised and concluded that it was not efficient as there was no evidence of disrupting attacks. The PCLOB also carried out a year-long study of the 702 programme, and found it is legal and clearly authorised by statute and that Section 702 has proven to be very effective including on terrorism issues. Finally, it acted on the transparency requirement and found that a number of classified facts did not need to be classified. The PCLOB is understood to report on the implementation of PPD-28 in the near future. In this regard, it considers that to retain information on a foreigner, the simple fact that that person is a foreigner is not enough.

The WP29 finally notes that EO12333 does not provide for any judicial review, oversight or redress mechanisms for the surveillance programmes conducted on its basis.

3.4.3 Conclusion

The draft adequacy decision demonstrates that a multi-layered approach of both internal and external oversight mechanisms is in place in the U.S. Even though the workings of the oversight mechanisms may be confusing, the WP29 is satisfied that, in general, sufficient internal oversight mechanisms are in place. The WP29, however, is concerned that there is insufficient oversight of the surveillance programmes undertaken on the basis of EO12333.

[54] PCLOB Report on the Surveillance Program Pursuant to Section 702 FISA, p. 24, 25

The WP29 notes that its previous criticism that the procedures in front of the FISC are not adversarial have only been mitigated to some extent by the introduction of the amici curiae who are tasked to "advance the protection of individual privacy and civil liberties". Nevertheless the FISC does not provide effective judicial oversight on the targeting of non-U.S. persons. Some doubts also remain regarding the ability of the FISC to effectively assess the targeting and minimisation procedures, as was also stated by the PCLOB.[55]

3.5 Guarantee D - Effective remedies need to be available to the individual

3.5.1 Judicial remedies

3.5.1.1 Standing requirement

The U.S. system relating to judicial remedies contains an important limit: the U.S. constitution requires an individual to demonstrate he has standing: "the requirement that plaintiffs have sustained or will sustain direct injury or harm and that this harm is redressable. At the Federal level, legal actions cannot be brought simply on the ground that an individual or group is displeased with a government action or law."[56] Such requirement appears to be nullified by the lack of notification to individuals subjected to surveillance even after these measures have ended. The CJEU and the ECtHR have repeatedly stated that individuals have to be able to access administrative or judicial redress. The ECtHR has confirmed in its Zakharov decision that based on the jurisprudence anyone can go to court if they have a legitimate reason to suspect an interference of their fundamental rights.[57]

Furthermore, foreigners located outside the U.S. are not offered full constitutional protection in the U.S., following jurisprudence from the Supreme Court of the United States[58]. This is true in particular in relation to the Fourth Amendment, which protects U.S. citizens – but not non-U.S. persons – against unreasonable searches and seizures, and from which much of the U.S. right to privacy is derived. European citizens and other European persons living outside the USA are simply excluded from the protection of the Fourth Amendment.[59]

The limited application of the Judicial Redress Act (both in terms of substance as it excludes national security but also in relation to the persons who can rely upon the law), the many exemptions and the legal uncertainty regarding the agencies to which the Judicial Redress Act will apply, do not satisfy the requirement to offer an effective redress mechanism to all individuals concerned in national security intelligence surveillance cases.

[55] PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA, p. 11
[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper v. Amnesty International USA
[57] ECtHR, Zakharov, §171
[58] U.S. v Verdugo - Urquidez , p. 264-266
[59] Report of the EU Co-Chairs, section 2

3.5.1.2 Presidential Policy Directive 28

The WP29 notes that PPD-28 is only a directive and therefore cannot create any rights for individuals. This can only be done through legislation. Therefore, individuals cannot go to court based on an alleged violation of the PPD-28 safeguards.

3.5.1.3 Foreign Intelligence Surveillance Act

Under the FISA, some remedies exist for individuals in case of unlawful surveillance. According to FISA, "an aggrieved person, other than a foreign power or an Agent of a foreign power [...], respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation". This however explicitly excludes the foreign power or Agent of a foreign power that was subject to the measure. Nevertheless, as already stated, the plaintiff will have to demonstrate he has standing which will not be possible in practice.

The USA Freedom Act has created an Amicus Curiae advisory panel to the FISA Court to give (optional) advice in case of significant new legal interpretation. Their task is however to provide unbiased advice, and not to defend the interest of a specific individual upon his/her request.

3.5.2 Administrative remedies

3.5.2.1 Inspectors-General

Another avenue for remedies is to go through the Inspector-General to whom a complaint can be filed. However, Inspectors-General do not have any obligation to look at every single complaint: there is no right to be heard, but rather a discretionary power. The Inspector-General can also issue reports with findings of violations where information are declassified. In case An individual could suppose the report affects him/her, he/she would then be able to go to court on the basis of the finding of the violation of the law.

3.5.2.2 Freedom of Information Act

A remedy available to all persons is the filing of a freedom of information request, based on the Freedom of Information Act (FOIA). According to the U.S. Government, a FOIA request can be made by generally any person – U.S. citizen or not – by simply asking for any agency record. This includes records on the individual, although in such a case it is required to provide a certification of identity. However, if information is classified to protect national security, it is unlikely a FOIA request will be successful, since an exemption applies: agencies are not obliged to provide access to classified information, including if this information relates to the individual who made the request. Information from ongoing law enforcement investigations is fully excluded from FOIA requests. Finally, in the WP29's understanding the FOIA request does not provide a right to have the legality of the processing checked by an independent authority.

3.5.3 Privacy Shield Ombudsperson

3.5.3.1 Establishment of an Ombudsperson

The Privacy Shield establishes a new mechanism 'for EU individuals' to submit requests regarding 'U.S. signals intelligence' to the newly created Privacy Shield Ombudsperson. The position of the Ombudsperson, as explained in the Memorandum annexed to the letter by Secretary of State John Kerry, dated 22 February 2016, will be filled by Under Secretary C. Novelli. She will serve in that function in addition to her role as the 'Senior Coordinator for International Information Technology Diplomacy', a role created in section 4(d) of PPD-28. It is stressed in the letter and in the Memorandum that the "Under Secretary reports directly to the Secretary of State, and is independent from the Intelligence Community".

Despite its name, it is explained in the Memorandum that the Privacy Shield Ombudsperson will not only process requests relating to national security access to data transmitted from the EU to the U.S. pursuant to the Privacy Shield, but also those where the data has been transmitted pursuant to Standard Contractual Clauses, Binding Corporate Rules, Derogations (under Article 26 of Directive 95/46/EC) or "possible future derogations", as defined in footnote 2 of the Memorandum.

The way the mechanism is supposed to work can be summarised in the following way: An EU individual submits a request to a Member State body competent for the oversight of national security services, or to a centralised 'EU individual complaint handling body', in case the latter will be created or designated. The authority forwarding the request to the Ombudsperson will have to check first whether the request is complete, as defined under 3(b) of the letter.[60] Once passed on to the Privacy Shield Ombudsperson and found in conformance with 3(b), the Privacy Shield Ombudsperson will provide a response, which means that he will finally confirm that "(i) the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executive orders, presidential directives, and agency policies, providing the limitations and safeguards described in the letter of the Office of the Director of National Intelligence (ODNI), have been complied with, or, in the event of non-compliance, such non-compliance has been remedied."[61] The response will "neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied."[62] As to the question how the investigation of

[60] b. The EU individual complaint handling body will ensure, in compliance with the following actions, that the request is complete:
(i) Verifying the identity of the individual, and that the individual is acting on his/her own behalf, and not as a representative of a governmental or intergovernmental organisation.
(ii) Ensuring the request is made in writing, and that it contains the following basic information:
• any information that forms the basis for the request,
• the nature of information or relief sought,
• the United States Government entities believed to be involved, if any, and
• the other measures pursued to obtain the information or relief requested and the response received through those other measures.
(iii) Verifying that the request pertains to data reasonably believed to have been transferred from the EU to the United States pursuant to the Privacy Shield, SCCs, BCRs, Derogations, or Possible Future Derogations.
(iv) Making an initial determination that the request is not frivolous, vexatious, or made in bad faith.
[61] Privacy Shield Annex III, section 4.e
[62] Privacy Shield Annex III, section 4.e

the Ombudsperson is carried out, it is explained that the Privacy Shield Ombudsperson "will work closely with other United States Government officials, including appropriate independent oversight bodies"[63], and more specifically, "will be able to coordinate closely with the ODNI, the Department of Justice, and other departments and agencies involved in United States national security as appropriate, and Inspectors General, Freedom of Information Act Officers, and Civil Liberties and Privacy Officers"[64]. This coordination shall be such to ensure that the Privacy Shield Ombudsperson can send a response including the confirmations as described above.

3.5.3.2 The assessment of the new Ombudsperson mechanism

The Working Party acknowledges the efforts made by the European Commission and the U.S. Government to introduce a new mechanism with a view to improving the possibilities of legal redress regarding U.S. surveillance activities. It understands that the assessment of this mechanism, as a novelty in international relations regarding signals intelligence or national security, is of particular importance.

In this section, the WP29 will assess how the establishment of the Privacy Shield Ombudsperson relates to the necessary requirements for individuals to seek legal redress, as have been laid down in the Charter, the ECHR and the jurisprudence of the European courts.

3.5.3.3 Can the establishment of an Ombudsperson per se be sufficient?

To start with, it needs be questioned whether the establishment of an "ombudsperson" can ever be considered to be in compliance with Article 47 Charter – which mentions an effective remedy before an impartial tribunal[65] – at least if no other avenue is available to seek effective legal redress. This is important because the CJEU, in Schrems, in its important consideration 95, refers to Article 47 Charter, and it does so without giving any indication that Article 47 is supposed to be understood with modifications in the context of surveillance measures. On the contrary the CJEU already applied Article 47 Charter in the Kadi II case[66] to measures of surveillance respectively of national respectively international security[67].

The jurisprudence of the ECtHR however makes very clear that legal redress to ordinary courts is not a condition to consider surveillance schemes to be compliant with Article 8 (and Article 13 of the ECHR).[68] Rather, the Court has developed under Article 8, as a necessary safeguard to surveillance activities, that redress before other authorities can be in order. The

[63] Privacy Shield Annex III, section 2.a
[64] Privacy Shield Annex III, section 2.a
[65] In the Explanations Relating to the Charter of Fundamental Rights, it is moreover stated that article 47 should be interpreted as providing a guarantee to the right to an effective remedy before a court (Explanation relating to the Charter of Fundamental Rights, Explanation on Article 47 (2007/C 303/02)).
[66] Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, European Commission and United Kingdom v. Kadi, 18 July 2013
[67] Kadi II §97 and 100: all Union acts, including those that are designed to give effect to resolutions adopted by the Security Counsel under Chapter VII of the Charter of the United Nations, are under review of lawfulness by the Courts of the European Union (Chapter VII is related to action with respect to threats to the peace, breaches of the peace, and acts of aggression).
[68] Article 13 of the ECHR obliges Member States to ensure that "everyone whose rights and freedoms (…) are violated shall have an effective remedy before a national authority". This does not necessarily need to be a judicial authority, as the ECtHR has clarified in Klass §56 and 67.

ECtHR nevertheless has high expectations of other authorities providing an effective remedy, stating that such an authority must be "independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise an effective and continuous control"[69].

In the Kennedy case and the Klass case the ECtHR provided insight in what these expectations might mean in the context of secret surveillance, when the data subject is not notified of the processing of his or her data. In both these judgements the authorities were considered as independent by the ECtHR, especially independent of the bodies carrying out the surveillance, but also independent from instructions[70] by any other authority. More specifically in the Kennedy case, the Court approved of an independent and impartial authority which had adopted its own rules of procedure and consisted of members that held or had held high judicial office or were experienced lawyers[71].

In undertaking its examination of complaints by individuals, the authorities in both judgments furthermore had access to all relevant information, including closed materials. Finally, both had the powers to remedy non-compliance.[72]

In addition to the question whether the Ombudsperson can be considered a 'tribunal', the application of Article 47 (2) Charter implies an additional challenge, since it provides that the tribunal has to be 'established by law'. It is doubtful however whether a Memorandum which sets forth the workings of a new mechanism can be considered 'law'.

As a consequence – with the principle of essential equivalency in mind – rather than assessing whether an Ombudsperson can formally be considered a tribunal established by law, the Working Party decided to elaborate further the nuances of the case law as regards the specific requirements necessary to consider 'legal remedies' and 'legal redress' compliant with the fundamental rights of Articles 7, 8 and 47 Charter and Article 8 (and 13) ECHR. In its further analysis, upon discussing the scope of application of the new mechanism, the Working Party will thus focus on the following criteria: the requirement to submit a request to the Ombudsperson and to receive a response ('standing'), the independence of the Ombudsperson, its investigatory power to access the necessary materials, including classified documents, and to request assistance from other agencies, and finally, its power to remedy non-compliance.

3.5.3.4 The scope of application of the Ombudsperson mechanism

With regard to access to the Ombudsperson mechanism, the WP29 considers all persons subject to EU law should be covered by the safeguards under the Privacy Shield. It would not be acceptable to make a distinction based on nationality, especially given that the fundamental rights in the EU apply to everyone, and not only to those holding an EU passport. Annex III

69 Klass § 56 and 67.
[70] ECtHR, Klass § 21 and 53.
[71] The G 10 Commission (at the time of the judgement) consists of three members, of which the Chairman must be qualified to hold judicial office, Klass § 21 and 53)
[72] ECtHR, Kennedy §167; Klass § 21 and 53.

refers to an 'EU individual' without further defining who that is. The Working Party regrets this uncertainty and suggests to provide for clarification in the sense that all persons subject to EU law have the right to have her or his request to the Ombudsperson processed according to the conditions of the Memorandum. Additionally, the Commission and the U.S. should address the question to what extent the Privacy Shield will also apply to citizens / residents of the countries of the EEA and Switzerland, which in the past did enjoy coverage by the Safe Harbour scheme.

Furthermore, the WP29 notes some uncertainty as to the scope of application of the Ombudsperson mechanism. Whereas the Memorandum provides that the Ombudsperson is charged with processing requests relating to national security to data transmitted from the EU to the U.S. pursuant to all transfer tools available under EU law, it is equally made clear in the Memorandum that it sets forth a mechanism "regarding signal intelligence". The latter term suggests that only such data transfers are covered where the data was collected by means of signal intelligence, which leads to the question whether data collected under FISA, e.g., is considered 'signals intelligence'. That appears to be the case as regards Section 702, as explained in the representation by the ODNI, p. 10.[73] However, the WP29 regrets that the use of the term 'signal intelligence' creates unnecessary uncertainty in this context.

As another consequence, it is the understanding of the Working Party that the Ombudsperson mechanism does not cover requests related to access by law enforcement agencies.[74] If so, it would remain unclear whether requests from some agencies, notably the CIA, would be covered by the mechanism.

3.5.3.5 'Standing' and the procedure of the request

To bring legal proceedings against surveillance measures by the U.S. Government before ordinary courts in the United States is very difficult. The Working Party is aware that the Supreme Court has denied standing in intelligence cases, where the applicant was not able to show individual "concrete, particularised, and actual or imminent or injury".[75] In this regard the establishment of the Ombudsperson is an important step, as it adds an avenue to some form of legal redress which would otherwise not be existing. The Working Party therefore welcomes the clarification in section 3(c). Based on this section, a demonstration that the requestor's data has in fact been accessed through signal intelligence activities is not needed in order to file a request under the new mechanism.

The Working Party largely endorses the procedure for identification of the complainant under the Ombudsperson mechanism. It makes perfect sense to have the identification take place on EU territory, as is also the case for the access mechanism under the EU-U.S. TFTP2 Agreement. However, the Working Party fails to understand why the verification in the EU should be carried out by the "Member States bodies competent for the oversight of national security services". In the first place, it seems unlikely that following article 4(2) Treaty on the

[73] Privacy Shield Annex VI, p. 10
[74] Memorandum on the establishment of an Ombudsperson, p.1
[75] Clapper v. Amnesty International USA, 568 U.S. ___ (2013) II. p.10

European Union, the European Commission would be in a position to attribute tasks to these bodies that clearly fall within the competence of the Member States.

Furthermore, given the variety of supervision mechanisms of national security services in Member States, the involvement of the corresponding authorities may seriously affect the effectiveness of the system for citizens in Member States. For instance, in cases where there are several authorities charged with the oversight of the national security services and it may be difficult for the individual to identify the relevant one, where the applicable national legal rules do not provide for the possibility that individuals may get into contact with the relevant supervisory body or where these authorities are not established in such a way that they are suited to carry out the tasks imposed on them in the draft adequacy decision[76]. Taking into account the involvement of DPAs in the application of and oversight on the Privacy Shield, as well as their similar role under the TFTP2 Agreement, it makes more sense to attribute this task to the national data protection authorities of the Member States. The Working Party underlines that it considers it to be unlikely that classified information would be processed as part of a procedure before the Privacy Shield Ombudsperson, since any reply will only be "compliant or non-compliant, but remedied".

3.5.3.6 Independence

The representations of the Secretary of State make clear that the position of the Ombudsperson will be carried out by an Under Secretary of the Department of State. He is nominated by the President and requires confirmation by the Senate. The role of Ombudsperson does not require additional confirmation; the allocation of the Ombudsperson's role suffices. The Under Secretary is nominated by the U.S. President, directed by the Secretary of State as the Ombudsperson, and confirmed by the U.S. Senate in her role as Under Secretary. As the letter and the Memorandum representations stress, the Ombudsperson is "independent from the U.S. Intelligence community". The WP29 however questions if the Ombudsperson is created within the most suitable department. Some knowledge and understanding of the workings of the intelligence community seems to be required in order to effectively fulfil the Ombudsperson's role, while at the same time indeed sufficient distance from the intelligence community is required to be able to act independent.

The Privacy Shield does not create specific criteria for the dismissal of the Ombudsperson. It is thus the understanding of the Working Party that the Ombudsperson can be dismissed in his role of Ombudsperson in the same way as he can be dismissed in his role of Under Secretary in the Department of State, which may potentially undermine the independent position of the Ombudsperson.

On its face, the designation of an Under Secretary in the State Department as an Ombudsperson is evidently different in terms of independence from establishing jurisdiction of an ordinary court for legal redress of an individual. The question is thus whether the Ombudsperson can be regarded, in terms of independence, as equal to other independent

[76] For example, in some EU Member States, individuals can only gain access to information held by the national security services through a request to a High Court Justice.

oversight bodies which have been found compliant. In the surveillance context, those would be in particular the Investigatory Powers Tribunal (IPT) in the UK and the G10 Commission in Germany.

Whether this is the case, needs to be additionally assessed by analysing the powers granted to the 'independent'.

3.5.3.7 Investigatory powers

In the Kadi II case the CJEU ruled in regard to Article 47 Charter that "the person concerned must be able to ascertain the reasons upon which the decision taken in relation to him is based, either by regarding the decision itself or by requesting and obtaining disclosure of those reasons, without prejudice to the power of the court having jurisdiction to require the authority concerned to disclose that information, so as to make it possible for him to defend his rights in the best possible conditions".[77] The Courts of the European Union are to ensure that that decision is taken on a sufficiently solid factual basis[78]. It states clearly that "the secrecy or confidentiality of […] information or evidence is no valid objection", at least not before the Courts of the European Union[79]. Therefore the Working Party concludes that the Ombudsperson must be given information and evidence that support the reasons relied on for conducting a measure, to meet the requirements of the CJEU[80].

It is as yet unclear what the extent of the investigatory powers of the Ombudsperson would be. Both the Commission draft decision and the Annex III from the State Department are not abundantly clear on this issue. As far as the Working Party understands, the Ombudsperson should get sufficient information in order to be able to state if a data processing operation by the security services takes place in accordance with the law, and if not, to make sure that the non-compliant situation is remedied. Neither the letter from the State Department nor the Commission draft decision however specify if the Ombudsperson would have direct access to the data held on the individual in question and can thus carry out his/her own investigation, or if he/she can only rely upon the reports from other U.S. Government officials.

3.5.3.8 Remedial powers

It remains rather unclear from the Memorandum in what way the Ombudsperson can order non-compliance to be remedied. In combination with the lack of clarity concerning the investigatory powers, it moreover remains unclear to what extent the Ombudsperson as such will be effectively capable of ordering non-compliance to be remedied and what the result of such an exercise would be. Could this mean data that was obtained in a non-compliant way (i.e. illegally) can no longer be used in any procedure and should be deleted?

[77] Kadi II §100.
78 Kadi II §119.
79 Kadi II §125.
[80] Kadi II §122; although the authority concerned does not have to produce all information and evidence underlying the reasons for a measure.

It is furthermore the understanding of the Working Party that the Privacy Shield does not provide for any appeal against or review of the "decision" by the Ombudsperson.

Finally when it comes to the communication of the Ombudsperson to the complainant after her examination of a complaint, the Ombudsperson must not reveal, if there has been any unlawfulness behaviour of the intelligence community. The answer provided will always be the same and it will be unspecific. In the Kadi II case the CJEU ruled that the competent authority (as a supervisory body) is obliged to state reasons that entail all circumstances, although Article 296 TFEU does not require a detailed response[81].

3.5.4 In conclusion

The existence of effective remedies for individuals remain a cause for concern for the WP29. First of all, the draft adequacy decision does not provide a clear answer to the question in what situations and under which preconditions individuals can bring a case in order to determine their rights..

The WP29 does recognise and welcome the introduction of an alternative redress mechanism in the form of the Ombudsperson, which is a unique development in the relations between the EU and a third country. Aside from the need to clarify the term 'EU individuals' as raised earlier, the mechanism creates an additional avenue for them to seek redress with the U.S. administration in order to ensure that any personal data of the applicant is processed in conformity with U.S. law.

At the same time, when assessing the Ombudsperson mechanism against the standards for an independent tribunal in the meaning of Article 47 Charter and the requirements the CJEU and ECtHR have established in its jurisprudence in surveillance cases, the WP29 notes significant deficiencies. First of all, concerns exist as to whether the Ombudsperson can be considered (formally and fully) independent, especially due to the relative ease with which political appointees can be dismissed. Secondly, concerns remain regarding the powers of the Ombudsperson to exercise effective and continuous control. Based on the available information in Annex III, the WP29 cannot come to the conclusion that the Ombudsperson will at all times have direct access to all information, files and IT systems required to make his own assessment nor that he can really compel the intelligence agencies in charge to end any non-compliant data processing, certainly in case of disagreement over the question if the data processing is in compliance with the law or not. Possibly, further clarification of the position and powers of the Ombudsperson can remove the concerns of the WP29.

3.6 Concluding remarks on safeguards and limitations applicable to U.S. national security authorities

The WP29 first of all commends the Commission and the U.S. authorities for all efforts that have been made to increase transparency on the effect that U.S. surveillance programmes may have on data transferred under the Privacy Shield – or any other transfer tool for that matter.

[81] Kadi II §116

Significant steps have been taken since the first Snowden revelations in June 2013. Nevertheless, the WP29 notes that concerns remain. At the very least additional explanations and clarifications of the rights and obligations under the Privacy Shield are required.

The two major concerns of the WP29 are the fact that massive and indiscriminate data collection is not fully excluded by the U.S. authorities and that the powers and position of the Ombudsperson have not been set out in more detail. Moreover, the national DPAs should be competent to initiate a procedure before the Ombudsperson on behalf of an individual, instead of the supervisory bodies for the intelligence agencies. In addition, although the WP29 certainly recognises the attempts to meet the concerns raised by the DPAs, further safeguards would be welcomed in order to ensure that any interferences that may be caused by the U.S. surveillance programmes are necessary in a democratic society.

4. Assessment of the law enforcement guarantees of the Privacy Shield

4.1 Introduction

With regard to public access to personal data for law enforcement purposes, the WP29 notes that the Privacy Principles in Annex II of the Privacy Shield contain a derogation that is identical to the derogation that was laid down in the Safe Harbour Privacy Principles. The general nature of the derogation has therefore been maintained, which means that the new Privacy Shield Principles enable interferences with the fundamental rights of the persons whose personal data is transferred from the EU to the U.S. "founded on national security and public interest requirements or on domestic legislation of the United States."[82]

One of the main criticisms brought by the Court to the Safe Harbour Decision in Schrems was however that it "does not contain any finding 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 European Union to the United States"

The WP29 therefore welcomes the effort of the U.S. administration to provide more insight into the legal framework regarding the interference with personal data transferred under the Privacy Shield for law enforcement purposes, including the applicable limitations and safeguards. At the same time, the WP29 underlines it regards the issue of public access bearing in mind the fact that any interference with the fundamental rights to private life and data protection need to be justifiable in a democratic society. The WP29 has therefore analysed the law enforcement guarantees of the Privacy Shield, using the framework as set out in Section 1.2 of this Opinion.

[82] Schrems, §87

4.2 Application of the European Essential Guarantees to access by law enforcement authorities to data held by corporations

4.2.1 Access by law enforcement authorities to personal data should be in accordance with the law and based on clear, precise and accessible rules

Annex VII to the Privacy Shield contains a letter from the U.S. Department of Justice, "providing a brief overview of the primary investigative tools used to obtain commercial data and other record information from corporations in the United States for criminal law enforcement or public interest (civil and regulatory) purposes, including the access limitations set forth in those authorities".

All procedures mentioned in Annex VII stem either from the U.S. Constitution directly (the Fourth Amendment), from statutory and procedural law or from Guidelines and Policies of the Department of Justice. However, Annex VII does not refer specifically to all the statutes that provide for these procedures, but instead focuses on describing in short the procedures themselves. Annex VII also mentions that "there are other legal bases for companies to challenge data requests from administrative agencies based on their specific industries and the types of data they possess", by giving several non-exhaustive examples such as the Bank Secrecy Act, the Fair Credit Reporting Act, the Right to Financial Privacy Act.

The WP29 notes that the framework of statutes, procedures and policies is fragmented and that the applicable legal basis to a given request for access will depend on the nature of the data sought, the nature of the company, the nature of the legal procedures (criminal, administrative, related to other public interest) and the nature of the entity requesting access.

Since all applicable rules to limit access by law enforcement authorities to data transferred under the Privacy Shield are based on the Constitution, on statutory law and on transparent policies of the Department of Justice, a presumption of accessibility of these rules is taken into account by the WP29. However, the clarity and precision of the rules can only be assessed in each individual type of procedure and request for access. The WP29 therefore regrets to note that, based on the available details in Annex VII to the Privacy Shield and the findings in the draft decision, such an assessment cannot be done at this moment.

4.2.2 Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

The WP29 duly notes that requesting access to data for law enforcement purposes can be considered to pursue a legitimate objective. For instance, Article 8(2) ECHR accepts interferences to the right to the protection for private life by a public authority "in the interests of (…) public safety, (…) for the prevention of disorder or crime". However, such interferences are only acceptable when they are necessary and proportionate[83].

[83] See the Working Document on the European Essential Guarantees, p. 7-9. For a general assessment of the concepts of necessity and proportionality, see WP29 "Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector", 27 February 2014.

According to the settled case-law of the CJEU, the principle of proportionality requires that the legislative measures proposing interferences with the rights to private life and to the protection of personal data "be appropriate for attaining the legitimate objectives pursued by *the legislation at issue* and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives"[84] (our emphasis). Therefore, the assessment of necessity and proportionality is always done in relation to a specific measure envisaged by legislation.

The U.S. authorities specify in Annex VII that federal prosecutors and federal investigative Agents are able to gain access to documents and other record information from organisations through "several types of compulsory legal processes, including grand jury subpoenas, administrative subpoenas, and search warrants" and may acquire other communications "pursuant to federal criminal wiretap and pen register authorities"[85]. In addition, agencies with civil and regulatory responsibilities may issue subpoenas to organisations for "business records, electronically stored information, or other tangible items"[86]. Annex VII furthermore specifies that these legal proceedings are used in general to obtain information from 'corporations' in the U.S., irrespective of whether they are certified or not within the Privacy Shield framework, and "without regard to the nationality of the data subject". In other words, it seems that the subjects of these protections are the organisations, and not the individuals themselves.

In addition to Annex VII, the draft decision – which is based on the Privacy Shield Principles – contains findings of the Commission regarding the existence in the U.S. of rules to limit interferences with the fundamental rights of the persons whose personal data are transferred from the EU to the U.S. under the Privacy Shield.

In particular, the findings in the draft decision refer to applicable limitations and safeguards under the Fourth Amendment of the U.S. Constitution, according to which searches and seizures by law enforcement authorities principally require a court-ordered warrant upon a showing of probable cause[87]. The findings also refer to the fact that in the exceptional cases where the warrant requirement does not apply, law enforcement is subject to a reasonableness test[88].

Nevertheless, the findings do not make it clear how these safeguards apply to non-U.S. persons. In fact, the draft decision acknowledges in a recital that "the protection under the Fourth Amendment does not extend to non-U.S. persons that are not resident in the United States"[89]. It is further stated in the same paragraphs of the draft decision that non-U.S. persons "benefit indirectly through the protection afforded to the U.S. companies holding the personal data and who are the recipients of law enforcement requests". The WP29 however regrets to note that this finding does not make any reference to a legal source, either in statutory law or case-law.

[84] Digital Rights Ireland, §46 and case-law cited therein.
[85] Annex VII, p. 2.
[86] Annex VII, p. 4.
[87] Draft adequacy decision, §107
[88] Privacy Shield, §107
[89] Draft adequacy decision, §108

All in all, the WP29 notes that the system of investigative tools used to obtain commercial data and other record information from corporations in the United States for criminal law enforcement or public interest purposes – including the access limitations and safeguards – is a complex environment of measures. Based on the information available, this system cannot be assessed in general at this moment. Specific assessment in individual cases is needed in order to truly assess the necessity and proportionality of the law enforcement investigative measures in relation to the fundamental rights to private life and data protection.

4.2.3 An independent oversight mechanism should exist

The WP29 duly notes the fact that most of the procedures described in Annex VII presuppose the involvement of a Court's decision before the authorities obtain access to data (e.g. court orders for Pen Register and Trap and Traces, court orders for surveillance pursuant to the Federal Wiretap Law, search warrants – Rule 41). However, it seems that not all of them require the a priori involvement of a Court. For instance, civil and Regulatory authorities "may issue subpoenas"[90]. In these cases, there is the possibility of an ex post judicial control of the reasonableness of the subpoena, as "a recipient of an administrative subpoena may challenge the enforcement of that subpoena in Court"[91].

Based on the available information, the WP29 notes that - with regard to access by law enforcement authorities to data held by companies in the U.S. a fairly robust independent oversight mechanism seems to be in place.

4.2.4 Effective remedies need to be available to the individual

As mentioned before, "The protection under the Fourth Amendment does not extend to non-U.S. persons that are not resident in the United States"[92]. This means that a non-U.S. person would not be able to challenge warrants or subpoenas in Court invoking the Fourth Amendment. The draft adequacy decision specifies that non-U.S. persons benefit indirectly through the protection afforded to the U.S. companies holding the personal data and who are the recipients of law enforcement requests. The WP29 however notes that, even if this protection were effective, it does not mean that effective remedies are available to individuals, since the subject of the right to an effective remedy in this scenario seems to be the company receiving the request of access, and not the individual whose data is at issue.

Annex VII does not contain any further information with regard to possible remedies stemming from statutory law which are available to non-U.S. persons when authorities or companies unlawfully provide or obtain access to the content of their data.

The WP29 welcomes the fact that the recently adopted Judicial Redress Act[93] provides for rights of judicial redress to non-U.S. persons. These rights are however limited to clearly defined causes of action: the right to obtain correction and access to data and attorney fees

[90] Annex VII, p. 4.
[91] Annex VII, p. 4.
[92] Draft adequacy decision, paragraph 108.
[93] Judicial Redress Act of 2015, H.R. 1428.

when a "designated Federal agency or component" denies amendment of data or denies access to such data and the right to obtain civil remedies in cases of disclosures of data "intentionally or wilfully made".

In addition, the U.S. case-law referred to in the footnotes of the relevant recitals of the draft decision, in particular City of Ontario v. Quon[94], Maryland v. King[95] and Samson v. California[96], is not relevant to assess whether non-U.S. persons can bring a claim to Court in order to challenge the lawfulness of an interference with their privacy[97]. All cases refer to the right to private life of U.S. persons, and all of them contain decisions of the U.S. Supreme Court that in fact limit the application of the Fourth Amendment.

All in all, the WP29 acknowledges and welcomes the adoption of the Judicial redress Act, but it remains doubtful whether effective remedies are actually available to individual data subjects.

4.3 Concluding remarks

The WP29 welcomes and recognises the effort of the U.S. administration to provide more insight into the legal framework regarding the interference with personal data transferred under the EU-U.S. Privacy Shield for law enforcement purposes, including the applicable limitations and safeguards.

The WP29 notes that the system of investigative tools of law enforcement authorities, including the applicable limitations and safeguards, is both extensive and complex and that the information included in the Privacy Shield is brief. The WP29 therefore regrets that, based on the limited information (i.e. in Annex VII to the Privacy Shield and on the findings in the draft decision) it is unable to provide a comprehensive assessment regarding the accessibility, foreseeability and the necessity and proportionality of the applicable rules at this time. Notwithstanding the other findings of the WP29 regarding the Privacy Shield in this Opinion, such an assessment might be part of an annual review of the Privacy Shield.

With regard to access by law enforcement authorities, the WP29 notes that a fairly robust independent oversight mechanism seems to be in place. Furthermore, the WP29 welcomes the adoption of the Judicial Redress Act, which grants rights of judicial redress to non-U.S. persons The WP29 however notes that these rights are of a limited nature. In addition to the finding that that a non-U.S. person would not be able to challenge warrants or subpoenas in Court invoking the Fourth Amendment, concerns remain whether effective remedies are actually available to individual data subjects in the area of law enforcement.

---

[94] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).
[96] *Samson v. California*, 547 U.S. 843, 848 (2006).
[97] In *Ontario v. Quon*, the Court held that the City of Ontario did not violate its employees' Fourth Amendment rights because the city's access to the content of the private messages of the employee in question was reasonable, as it was motivated by a legitimate work related purpose and was not excessive in scope. In *Samson v. California*, the Court found that "the Fourth Amendment does not prohibit a police officer from conducting a suspicionless search of a parolee". In *Maryland v. King*, the Court held that when officers make an arrest supported by probable cause to hold a suspect for a serious offense and bring him to the station to be detained in custody, taking and analysing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment.

5. CONCLUSIONS AND RECOMMENDATIONS

The WP29 first of all welcomes the fact that within five months after the invalidation of the Safe Harbour a new draft adequacy decision was presented, containing many improvements compared to the previous mechanism. It is particularly pleased with the increased transparency that is offered through the introduction of two Privacy Shield Lists on the website of the DoC: one list containing the records of those organisations adhering to the Privacy Shield, and one list containing the records of those organisations that have adhered to the Shield in the past, but no longer do so. The increased transparency in relation to public access to data transferred under the Privacy Shield, either for national security or law enforcement purposes, is also welcomed. Finally, the WP29 is very pleased to learn that all data transfers to the U.S. will henceforth be given the same protection: there are no specific legal provisions in place to give advantage to one tool or another.

5.1 Three points of concern

However, three major points of concern do remain, that in the view of the WP29 will need to be addressed.

The first concern is that the language used in the draft adequacy decision does not oblige organisations to delete data if they are no longer necessary. This is an essential element of EU data protection law to ensure that data is kept for no longer than necessary to achieve the purpose for which the data were collected. Secondly, the WP29 understands from Annex VI that the U.S. administration does not fully exclude the continued collection of massive and indiscriminate data. The WP29 has consistently held that such data collection, is an unjustified interference with the fundamental rights of individuals. The third point of concern regards the introduction of the Ombudsperson mechanism. Even though the WP29 welcomes this unprecedented step creating an additional redress and oversight mechanism for individuals, concerns remain as to whether the Ombudsperson has sufficient powers to function effectively. As a minimum, both the powers and the position of the Ombudsperson need to be clarified in order to demonstrate that the role is truly independent and can offer an effective remedy to non-compliant data processing.

5.2 Recommended clarifications

In addition to the points mentioned above, the WP29 has indicated various points throughout this Opinion where further clarification of the adequacy decision is in order. Most importantly, this regards the need to ensure that the key data protection notions used in the Privacy Shield are defined and applied in a consistent way. This is currently not the case. The introduction of a glossary of terms in the Privacy Shield F.A.Q., with definitions ideally agreed between the EU and the U.S., would be welcomed. The WP29 also concludes that onward transfers of EU personal data are insufficiently framed, especially regarding their scope, the limitation of their purpose and the guarantees applying to transfers to Agents. As regards the access to Privacy Shield data by law enforcement, especially to foreseeability of the legislation is a concern, due to the extensive and complex nature of the U.S. law

enforcement system at both Federal and state level, and the limited information included in the adequacy decision.

The Privacy Shield is the first adequacy decision that has been drafted since the texts of the GDPR were agreed in principle. Still, many of the improvements on the level of data protection offered to individuals are not reflected in the Privacy Shield. The WP29 therefore recommends that a review of this adequacy decision, as well as of the adequacy decisions issued for other third countries, should take place shortly after the GDPR enters into application.

A final recommendation of the WP29 to be highlighted here regards the joint review. The WP29 welcomes the fact that the Privacy Shield adequacy decision will indeed be reviewed on a yearly basis, with a broad involvement of DPAs and other relevant parties. It would welcome agreement on the elements of the joint reviews, including on the drafting and presentation of the review report by all parties well in advance of the first review.