Chuck, Michele, Susan and Lisa,

Please see below my review of possible requirements contained within the Article 29 Data Protection Working Party Opinion 01/2016 on the EU – U.S. Privacy Shield.

UP Users/Purposes

[UP-D2-R1]

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. pg 4

[UP-D2-R2]

The requirement for a third country to ensure an adequate level of data protection was further defined by the CJEU in Schrems…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” pg.10

[UP-D2-R3]

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’. The WP29 tried to find the equivalent safeguards **which ensure a level of 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**. pg 11 (emphasis added)

[UP-D2-R4]

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.pg 11

[UP-D2-R5]

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** for intelligence activities:

[UP-D2-R6]

1. 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;

[UP-D2-R7]

1. 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;

[UP-D2-R8]

1. 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;

[UP-D2-R9]

1. Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body. pg. 12

[UP-D2-R10]

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. pg. 12

[UP-D2-R11]

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 organization 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.pg 16

[UP-D2-R12]

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 security12, 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. pg. 17

[UP-D2-R13]

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.pg 17

[UP-D2-R14]

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. 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. pg. 20

[UP-D2-R15]

It should be clarified that in any case, the Choice principle cannot be used to circumvent the Purpose limitation principle19. 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.pg 20

[UP-D2-R16]

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. pg 21

[UP-D2-R17]

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. pg 21

[UP-D2-R18]

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.pg.38

[UP-D2-R19]

the WP29 recalls that it has consistently considered that massive and indiscriminate collection of data in any case cannot be regarded as proportionate.pg. 39

[UP-D2-R20]

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…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. pg.40

[UP-D2-R21]

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. pg.53

[UP-D2-R22]

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 momentpg.pg 53

[UP-D2-R23]

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 pg.53

[UP-D2-R24]

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. pg. 54

[UP-D2-R25]

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 pg.57

GA Gated Access

[GA-D2-R1]

The requirement for a third country to ensure an adequate level of data protection was further defined by the CJEU in Schrems…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” pg.10

[GA-D2-R2]

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.pg 11

[GA-D2-R3]

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.pg 11

[GA-D2-R4]

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** for intelligence activities:

[GA-D2-R5]

1. 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;

[GA-D2-R6]

1. 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;

[GA-D2-R7]

1. 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;

[GA-D2-R8]

1. Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body. pg. 12

[GA-D2-R9]

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. pg 13

[GA-D2-R10]

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 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.pg 18

[GA-D2-R11]

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. pg.53

[GA-D2-R12]

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 momentpg.pg 53

[GA-D2-R13]

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. pg. 54

DA Data Accuracy

[DA-D2-R1]

The Data Integrity and Purpose Limitation principle (Annex II, II.5) also states: “To thecextent 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.pg24

DE Data Elements

[DE-D2-R1]

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’. The WP29 tried to find the equivalent safeguards **which ensure a level of 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**. pg 11 (emphasis added)

[DE-D2-R1]

**Proportionality:** 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.

[DE-D2-R2]

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.pg 11

[DE-D2-R3]

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. pg. 12

[DE-D2-R4]

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. pg 13

[DE-D2-R5]

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 pg. 14

[DE-D2-R6]

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 pg 15

[DE-D2-R7]

the individual must receive both confirmation that data are being processed regarding him and communication of the data processed. pg15

[DE-D2-R8]

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. pg17

[DE-D2-R9]

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.pg.38

[GA-D2-R10]

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. pg. 54

PR Privacy

[PR-D2-R1]

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. pg 3

[PR-D2-R2]

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. pg 3

[PR-D2-R3]

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. pg.3

[PR-D2-R4]

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 pg 3

[PR-D2-R5]

The requirement for a third country to ensure an adequate level of data protection was further defined by the CJEU in Schrems…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” pg.10

[PR-D2-R6]

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’. The WP29 tried to find the equivalent safeguards **which ensure a level of 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**. pg 11 (emphasis added)

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.pg 11

[PR-D2-R7]

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** for intelligence activities:

[PR-D2-R8]

1. 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;

[PR-D2-R9]

1. 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;

[PR-D2-R10]

1. 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;

[PR-D2-R11]

1. Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body. pg. 12

[PR-D2-R12]

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 pg. 14

[PR-D2-R13]

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. pg 15

[PR-D2-R14]

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 security12, 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. pg. 17

[PR-D2-R15]

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. 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. pg. 20

[PR-D2-R16]

It should be clarified that in any case, the Choice principle cannot be used to circumvent the Purpose limitation principle19. 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.pg 20

[PR-D2-R17]

The WP29 would like to emphasise that aggregated data can still be re-identified and therefore should be regarded as personal data. pg 36

[PR-D2-R18]

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”(our emphasis). Therefore, the assessment of necessity and proportionality is always done in relation to a specific measure envisaged by legislation. pg. 54

CX Coexistence

[CX-D2-R1]

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 pg3

[CX-D2-R2]

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.pg 11

[CX-D2-R3]

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. pg 13

CM Compliance

[CM-D2-R1]

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. pg 3

[CM-D2-R2]

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. pg 3

[CM-D2-R3]

The requirement for a third country to ensure an adequate level of data protection was further defined by the CJEU in Schrems…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” pg.10

[CM-D2-R4]

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’. The WP29 tried to find the equivalent safeguards **which ensure a level of 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**. pg 11 (emphasis added)

[CM-D2-R5]

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. pg 12

[CM-D2-R6]

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. pg. 12

[CM-D2-R7]

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. pg 13

[CM-D2-R8]

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 pg. 14

[CM-D2-R9]

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 security12, 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. pg. 17

[CM-D2-R10]

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).pg 21

[CM-D2-R11]

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. pg. 30

SM System Model

[SM-D2-R1]

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.pg 4

[SM-D2-R2]

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.pg 11

[SM-D2-R3]

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** for intelligence activities:

[SM-D2-R4]

1. 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;

[SM-D2-R5]

1. 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;

[SM-D2-R6]

1. 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;

[SM-D2-R6]

1. Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body. pg. 12

[SM-D2-R7]

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. pg. 12

[SM-D2-R8]

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. pg 13

SM-D2-R9

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 nonU.S. persons that are not resident in the United States” 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**. pg 55

CS Cost

[CS-D2-R1]

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. pg 12

BE Benefits

[BE-D2-R1]

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. pg 12

RI Risks

[RI-D2-R1]

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 pg 3

[RI-D2-R2]

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.pg 4

[RI-D2-R3]

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.pg 11

[RI-D2-R4]

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. pg 13

[RI-D2-R5]

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. pg. 30