EUROPEAN
COMMISSION

Brussels, 29.4.2016
COM(2016) 237 final

2016/0126 (NLE)

Proposal for a

COUNCIL DECISION

on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

A High Level Contact Group ("HLCG"), composed of senior officials from the Commission, the Council Presidency and the U.S. Departments of Justice, Homeland Security and State, was established in November 2006 to explore ways that would enable the EU and the U.S. to work more closely and efficiently together in the exchange of law enforcement information while ensuring that the protection of personal data and privacy are guaranteed. The conclusion reached in the HLCG final report of October 2009[1] was that an international agreement binding both the EU and the U.S. to apply agreed common data protection principles for transatlantic data transfers in the law enforcement area was the best option: it would offer the advantage of establishing the fundamentals of effective privacy and personal data protection governing any exchange of law enforcement information and would provide the highest level of legal certainty.

On 3 December 2010, the Council adopted a decision authorising the Commission to open negotiations on an agreement between the European Union and the United States of America on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters (hereinafter referred to as "the Umbrella Agreement").[2]

On 28 March 2011, the Commission opened negotiations. On 8 September 2015, the Parties initialled the text.

The Umbrella Agreement establishes (for the first time ever) a comprehensive framework of data protection principles and safeguards when personal information[3] is transferred for criminal law enforcement purposes between the U.S., on the one hand, and the EU or its Member States on the other. The double objective is to ensure a high level of data protection and, thereby, enhance cooperation between the parties. Whilst not being itself the legal basis for any transfer of personal information to the U.S., the Umbrella Agreement supplements, where necessary, data protection safeguards in existing and future data transfer agreements or national provisions authorising such transfers.

This represents a very substantial improvement compared to the present situation where personal information is transferred across the Atlantic on the basis of legal instruments

---

1 Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection, Brussels, 23 November 2009, 15851/09, JAI 822 DATAPROTECT 74 USA 102.

2 Together with the adoption of the EU data protection reform and the new "EU-U.S. Privacy Shield" concerning data transfers in the commercial area, the conclusion of a meaningful and comprehensive Umbrella Agreement is a core element of the strategy set out in the Commission's Communication on Rebuilding Trust in EU-U.S. Data Flows (COM(20123) 846) of 27 November 2013, available at http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf, as also reaffirmed in President Juncker's Political Guidelines, and in the Communication from the Commission to the European Parliament and the Council "Transatlantic Data Flows: Restoring Trust through Strong Safeguards", COM(2016) 117 final of 29 February 2016, available at: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.

3 The term "personal information" as used in the Umbrella Agreement is synonym to the EU concept pf "personal data".

(international agreements or domestic laws) that generally contain no or only weak data protection provisions.

- **Consistency with existing policy provisions in the policy area**

The Umbrella Agreement will enhance the protections afforded to all personal data of EU data subjects when exchanged with the U.S. for criminal law enforcement purposes. By establishing a comprehensive framework of data protection guarantees, the Agreement will complement existing agreements (both bilateral agreements between and Member States and the U.S. and EU-U.S. agreements) on the basis of which personal data is sent to the U.S. for law enforcement purposes, when and to the extent they lack the requisite level of protections and safeguards.

Moreover, the Agreement will provide a "safety net" for future EU/Member States-U.S. agreements below which the level of protection cannot fall. This is an important guarantee for the future and a major shift from the present situation where safeguards, protections and rights have to be negotiated afresh for each individual new agreement.

Overall, the Umbrella Agreement will bring significant added value in terms of raising the level of protection of EU data subjects, in line with the requirements of EU primary and secondary law. For the very first time, it will introduce a data protection instrument that covers in a comprehensive and consistent manner all data transfers in a given area (i.e. transatlantic data exchanges in the field of police cooperation and judicial cooperation in criminal matters). Furthermore, the Umbrella Agreement will substantiate in the transatlantic context the general requirements on international data transfers laid down in the future Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (hereinafter "the Police Directive")[4] adopted on 14 April 2016. In light of the above, the Umbrella Agreement also sets an important precedent for possible similar agreements with other international partners.

- **Consistency with other Union policies**

The Umbrella Agreement is expected to have a significant impact on police and law enforcement cooperation with the United States. By establishing a common and comprehensive framework of data protection rules and guarantees, it will enable the EU or its Member States, on the one hand, and U.S. criminal law enforcement authorities on the other hand to cooperate more effectively with each other. Moreover, it will ensure that existing agreements contain all necessary protections. This will enable continuity in law enforcement cooperation while ensuring greater legal certainty when transfers are made. The Agreement will also facilitate the conclusion of future data transfer agreements with the U.S. in the criminal law enforcement sector, as data protection safeguards will have been agreed and will thus not have to be negotiated again and again. Finally, setting common standards in this key but complex area of cooperation is an important achievement that can significantly contribute to restoring trust in transatlantic data flows.

[4] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM/2012/010 final - 2012/0010 (COD), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=en

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis for this proposal is Article 16 TFEU, in conjunction with Article 218 (6)(a) TFEU.

• Subsidiarity

The Umbrella Agreement falls under the exclusive competence of the EU pursuant to Article 3(2) TFEU. Therefore, the subsidiarity principle does not apply.

• Proportionality

The Umbrella Agreement provides for the data protection guarantees required under the Negotiating Directives of the Council. They are considered as necessary elements to ensure the requisite level of protection when personal data is transferred to a third country, both under the Charter of Fundamental Rights and under the evolving EU acquis. Neither a substantially smaller catalogue of such guarantees nor an instrument with less binding force could be considered as sufficient to provide such a level of protection. Therefore, the proposal does not go further than what is necessary to achieve the policy objective of establishing a framework for the protection of personal data when transferred between the United States, on the one hand, and the European Union or its Member States, on the other, in the context of law enforcement.

• Choice of the instrument

The establishment of a binding framework for the protection of personal data, that will complement existing agreements and constitute a baseline for future agreements, can only be ensured through an international agreement concluded between the EU and the United States.

Moreover, as highlighted in the HLCG report of October 2009, an international agreement provides the highest level of legal certainty.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

• Ex-post evaluations/fitness checks of existing legislation

Not applicable.

• Stakeholder consultations

The Commission has regularly reported both orally and in writing to the designated special Council committee on the progress of the negotiations. The European Parliament has been regularly informed, through its Committee for Civil Liberties, Justice and Home Affairs (LIBE), both orally and in writing.

• Collection and use of expertise

The initiative implements the Council negotiation directives of 3 December 2010.

• Impact assessment

No impact assessment was needed. The proposed agreement is in line with the Council negotiating directives.

- **Regulatory fitness and simplification**

Not applicable.

- **Fundamental rights**

The provisions of the Umbrella Agreement aim at the protection of the fundamental right to the protection of personal data and the right to an effective remedy and to a fair trial, as enshrined, respectively, in Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union.

4. BUDGETARY IMPLICATIONS

The proposed agreement has no budgetary implications.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

Implementation by Member States will be necessary, but no major changes in the laws are to be expected since the substantive provisions of the Umbrella Agreement reflect to a large extent rules that are already applicable to EU and national authorities under EU and/or national law.

- **Detailed explanation of the specific provisions of the proposal**

The Umbrella Agreement, in line with the Council negotiating directives, covers five categories of provisions: (i) horizontal provisions; (ii) data protection principles and safeguards; (iii) individual rights; (iv) aspects relating to the application of the Agreement and to oversight; and (v) final provisions.

(i) Horizontal Provisions

(i) Purpose of the Agreement (Article 1)

To attain the purpose of the agreement (*i.e.* to ensure a high level of protection of personal information and to enhance cooperation in the law enforcement area), the Umbrella Agreement establishes a framework for the protection of personal information when transferred between the U.S., on the one hand, and the EU or its Member States on the other, for the prevention, investigation, detection or prosecution of criminal offences, including terrorism. The reference to the notions of "prevention, detection, investigation and prosecution of criminal offences" (hereinafter collectively referred to as "law enforcement") ensures that this agreement will be compatible with the architecture of the current and future EU data protection *acquis* (in particular, the delineation between the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation"[5]) and the "Police Directive" as regards their respective coverage).

By specifying that the Umbrella Agreement in itself shall not be the legal basis for any transfer of personal information and that a (separate) legal basis shall always be required,

[5] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final 2012/0011 (COD), available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Article 1 also makes clear that the Umbrella Agreement is a genuine fundamental right agreement establishing a set of protections and safeguards applying to such transfers.

(ii) Definitions (Article 2)

The key terms of the Umbrella Agreement are defined in Article 2. The definitions of "personal information", "processing of personal information", "Parties", "Member State" and "Competent Authority" are substantially in line with how these concepts have been defined in other EU-U.S. agreements and/or in the EU data protection *acquis*.

(iii) Scope of the Agreement (Article 3)

Article 3 of the Umbrella Agreement defines the scope of the Umbrella Agreement. It will ensure that the protections and safeguards provided by the Umbrella Agreement apply to all data exchanges taking place in the context of transatlantic law enforcement co-operation in criminal matters. This includes transfers on the basis of domestic laws, EU-U.S. agreements (e.g. the EU-U.S. Mutual Legal Assistance Treaty), Member States-U.S. agreements (e.g. Mutual Legal Assistance Treaties, Agreements on Enhancing Cooperation in Preventing and Combating Serious Crime, Terrorist Screening Information Agreements or Arrangements), as well as specific agreements providing for the transfer of personal data by private entities for law enforcement purposes (e.g. under the EU-U.S. Passenger Name Records[6] ("PNR") Agreement and the Terrorist Finance Tracking Program[7] ("TFTP") Agreement). The scope is formulated on a "data transfer basis", *i.e.* it covers, in principle, all data transfers for criminal law enforcement purposes between the EU and the U.S. regardless of the nationality or place of residence of the data subject concerned.

The Umbrella Agreement will not cover transfers of personal data (or other forms of cooperation) between U.S. and Member States' authorities responsible for safeguarding national security.

(iv) Non-discrimination (Article 4)

Article 4 provides that each Party will implement the Umbrella Agreement without any arbitrary or unjustifiable discrimination between its own nationals and those of the other Party.

This Article complements and strengthens other provisions of the Agreement (in particular, articles providing safeguards to individuals such as access, rectification and administrative redress, see *infra*), as it ensures that European nationals will benefit, in principle, from equal treatment with U.S. citizens when it comes to the practical implementation of these provisions by U.S. authorities.

(v) Effect of the Agreement (Article 5)

[6] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ of 11.8.2012, L 215/5.

[7] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ of 27.7.2010, L 195/5.

As regards existing agreements in place between the EU/Member States and the U.S., the Umbrella Agreement will supplement them as appropriate *i.e.* when and to the extent they lack the necessary data protection safeguards.[8]

The effective implementation of the Umbrella Agreement (and in particular of its articles concerning individual rights) triggers a presumption of compatibility with the applicable international data transfer rules. This is neither an automatic nor a general presumption and, like all presumptions, it can be rebutted. It is not an automatic presumption because its application expressly depends on the effective implementation of the Umbrella Agreement by the U.S. and more specifically – as paragraph 2 of Article 5 expressly clarifies – on the effective implementation of the articles on the rights of individuals (in particular, access, rectification, administrative and judicial redress). It is not a general presumption either: given that the Umbrella Agreement is not a "self-standing" instrument for transfers, such a presumption necessarily operates on a "case by case" basis, *i.e.* by assessing if the combination of the Umbrella Agreement and the specific legal basis for the transfer provide a level of protection in line with EU data protection rules. . In other words, differently from an adequacy finding, this clause does not provide for an "en bloc" recognition of the level of protection provided in the U.S. as such or a general authorisation for transfers.

(ii) Data Protection Principles and Safeguards

The Articles described below cover important principles governing personal data processing as well as key safeguards and limitations.

(i) Purpose and Use Limitations (Article 6)

In line with the EU Charter of Fundamental Rights and the EU *acquis*, Article 6 applies the purpose limitation principle to all transfers of personal data covered by the Umbrella Agreement, both in case of transfers in relation to specific cases and where the U.S. and the EU/its Member States conclude an agreement that authorises transfers of personal data in bulk. Processing (which includes transfers) can take place only for explicit and legitimate purposes within the scope of the Umbrella Agreement, *i.e.* the prevention, investigation, detection or prosecution of criminal offences, including terrorism.

Moreover, further processing of personal information by other (law enforcement, regulatory or administrative) authorities than the first receiving authority of a Party is allowed on condition that it is not incompatible with the purposes for which it was originally transferred and that such other authority complies with all the other provisions of the Umbrella Agreement.

The transferring competent authority may also impose additional conditions (e.g. on the use of the data) in specific cases.

Finally, personal information shall only be processed if "directly relevant to and not excessive or overbroad in relation to the purposes of such processing".

[8] The fourth recital in the Preamble indicates that the Umbrella Agreement shall not alter, condition or otherwise derogate from agreements in which it is established that they provide an adequate level of data protection, with the exception of the judicial redress provision in Article 19, which will also apply to them. This concerns the PNR and TFTP agreements.

Article 6 is a key provision of the Agreement: it ensures the application of the safeguards to the entire "life cycle" of a given data set from the original transfer from the EU to its processing by a U.S. competent authority and vice-versa, as well as its possible further sharing with/processing by another U.S. authority or, in the case of a data transfer from the U.S. to a competent authority of the EU or (one of) its Member States, its possible further sharing with/processing by another EU or Member State authority.

(ii) Onward Transfer (Article 7)

The onward transfer limitations set out in Article 7 entail that in case a U.S. authority intends to further transfer data it has received from the EU or one of its Member States to a third country/international organisation not bound by the agreement, it will first have to obtain the consent from the law enforcement authority in the EU which has originally transferred the data to the United States. This rule equally applies in case an authority of the EU or one of its Member States intends to further transfer data it has received from the U.S. to a third country/international organisation.

When deciding to grant its consent, the original transferring authority will have to take into due account all relevant factors, including the purpose for which the data was initially transferred and whether the third country or international organisation offers an appropriate level of protection of personal information. It may also subject the transfer to specific conditions.

Furthermore, as for the articles on purpose limitation (see *supra* Art. 6), retention periods (see *infra* Art. 12) and sensitive data (see *infra* Art. 13), this Article expressly takes into account the special sensitivity of the transfer in bulk of data of unsuspected persons (e.g. PNR data of every passenger taking a flight, independently of any specific suspicion), in that it requires that any further transfer of personal information "other than in relation to specific cases" may only take place under specific conditions set forth in the agreement that provide due justification for the onward transfer.

The specific situation of onward transfers to another State within the EU (e.g. the French police sharing with the German police information received from the U.S. FBI) is also addressed in this Article (par. 4) by providing that if under applicable rules such transfers are subject to prior consent, the authority which has originally sent the information (e.g. the U.S. FBI) will not be able to refuse consent or impose conditions on data protection grounds (as all the authorities involved are bound by the Umbrella Agreement).

(iii) Data Quality and Integrity of Information (Article 8)

The Parties will take reasonable steps to ensure that transferred personal data is maintained with such accuracy, relevance, timeliness and completeness as is necessary and appropriate for lawful processing of the information. Where the receiving or transferring authority becomes aware of significant doubts as to the relevance, timeliness, completeness or accuracy of personal data received or transferred, it shall, where feasible, advise the transferring/receiving authority thereof.

(iv) Information Security (Article 9) and Notification of an information security incident (Article 10)

These articles contribute to ensuring a high level of security of personal data exchanged by the parties to the Umbrella Agreement.

First, pursuant to Article 9, appropriate technical, security and organisational arrangements will be put in place by the Parties for the protection of personal information against accidental or unlawful destruction, accidental loss, and unauthorised disclosure, alteration, access or other processing. These arrangements will also include that access to personal data be granted only to authorised staff.

Secondly, pursuant to Article 10, in case of a security incident presenting a significant risk of damage, appropriate action shall be promptly taken to mitigate the damage, including notification to the transferring authority and, where appropriate given the circumstances of the incident, the individual concerned. Exceptions to the notification obligation are exhaustively listed in the provision and correspond to reasonable limitations (e.g. national security).

(v) Maintaining records (Article 11)

The Parties shall have in place effective methods (such as logs) for demonstrating the lawfulness of processing and use of personal information.

This requirement represents a significant safeguard for individuals, as it puts the onus on law enforcement authorities to demonstrate that a given data processing operation was carried out in accordance with the law. The obligation to document data processing operations entails, in particular, that there will be a "trace" in case of unlawful processing. This should facilitate the handling of complaints and the introduction of claims regarding the lawfulness of the processing operations.

(vi) Retention period (Article 12)

The processing of data will be subject to specific retention periods in order to ensure that data will not be retained for longer than necessary and appropriate. To determine the duration of these retention periods, a number of elements will have to be taken into account, in particular the purpose of processing or use, the nature of the data and the impact on the rights and interests of the data subjects concerned.

It is also specified that, where the Parties conclude an agreement on the transfer of "bulk data", such agreement must contain a specific provision on the applicable retention period. With this provision, the Parties accept the principle that such bulk transfer agreements shall contain a specific retention period, which therefore will not have to be negotiated again.

The retention periods will be subject to periodic reviews to determine whether changed circumstances require any modification of the applicable period.

To ensure transparency, retention periods will have to be published or otherwise made publicly available.

(vii) Special categories of data (Article 13)

The processing of personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, trade-union membership or personal information concerning health or sexual life, may only take place when appropriate safeguards are in place in accordance with law (e.g. masking the information after effecting the purpose for which the data was processed or requiring supervisory approval to access the information).

Agreements allowing the "bulk transfer" of personal data will have to further specify the standards and conditions under which special categories of data can be processed.

The provisions on special categories of data are coherent with the requirement that processing shall be directly relevant and not excessive under Article 6 on purpose and use limitations.

(viii) Automated decision-making (Article 15)

Data processing that may result in decisions having negative consequences on an individual (e.g. in the context of profiling) may not be based solely on the automated processing of personal information, unless authorised by domestic law, and provided that appropriate safeguards are in place, including the possibility to obtain human intervention.

(ix) Transparency (Article 20)

Individuals are entitled to receive information (through general or individual notices and subject to "reasonable restrictions") regarding the purpose of processing and possible further use of their personal data, the laws or rules under which such processing takes place, the identity of third parties to whom their personal information may be disclosed, as well as the access, rectification and redress mechanisms available.

To raise the individuals' awareness as to why and by whom their data is processed contributes to the possibility for individuals to exercise their rights to access, rectification or redress (see *infra* Art. 16-19).

(iii) Individual Rights

These rights are of particular relevance for the protection of data subjects who will be able, for the first time, to avail themselves of rights of general application for any transatlantic transfer of personal data in the criminal law enforcement sector.

(i) Access and Rectification (Article 16 and Article 17)

The right to access entitles any individual to seek and obtain access to his or her personal data. The grounds for restricting access are set out exhaustively and correspond to reasonable restrictions (e.g. safeguard national security, avoid prejudicing the investigation or prosecution of criminal offenses, protect the rights and freedoms of others). Excessive expenses may not be imposed as a condition to access one's data.

The right to rectification entitles any individual to request the correction or rectification of his or her personal data in case it is either inaccurate or it has been improperly processed. This may include supplementation, erasure, blocking or other measures or methods for addressing inaccuracies or improper processing.

Where the competent authority of the recipient country concludes, following a request by an individual, a notification by the provider of the personal information or its own investigation, that the information is inaccurate or has been improperly processed, it shall take measures of supplementation, erasure, blocking, or other measures of correction or rectification.

Where permitted by national law, any individual is entitled to authorise, an oversight authority (*i.e.* a national data protection authority for an EU data subject) to request access or rectification on his or her behalf. This possibility of the indirect exercise of rights, through an

authority and within a legal system they are familiar with, should concretely assist the data subjects when seeking to enforce their rights.

If access or rectification requests are denied or restricted, the requested authority shall provide the individual (or his or her duly authorised representative) with a response setting forth the reasons for the denial or restriction of access or rectification. The obligation to provide the individual with a reasoned reply aims at enabling and facilitating the exercise of his/her right to administrative and judicial redress in case access/rectification is denied or restricted by the concerned law enforcement authority.

(ii) Administrative redress (Article 18)

Should an individual disagree with the outcome of his or her request for access/rectification of personal data, he or she will be entitled to seek administrative redress. As for access and rectification, to facilitate the effective exercise of this right, the data subject concerned is entitled to authorise an oversight authority (*i.e.* a national data protection authority for an EU data subject) or another representative, where permitted under applicable domestic law.

The authority from which relief is sought will provide the data subject concerned with a written response indicating, where applicable, the ameliorative or corrective actions taken.

(iii) Judicial Redress (Article 19)

The citizens of each Party shall be able to seek judicial redress for the i) denial of access, ii) denial of rectification or iii) unlawful disclosure by the authorities of the other Party.

On the U.S. side, this has been reflected in the Judicial Redress Act signed by President Obama on 24 February 2016. This Act will extend to the citizens of "covered countries"[9] these three judicial redress grounds as provided under the 1974 US Privacy Act, but currently reserved to U.S. citizens and permanent residents. The fourth recital of the Umbrella Agreement's Preamble makes clear that this extension will also cover data exchanged under agreements such as PNR and TFTP. In combination with the adoption of the Judicial Redress Act, Article 19 will thus significantly improve the judicial protection of EU citizens.

Although the Judicial Redress Act contains a number of limitations (in particular, it will only apply to the data of citizens from "covered countries" whose data have been transferred by EU law enforcement authorities, in particular, but not only EU citizens), Article 19 of the Umbrella Agreement addresses a long-sought EU demand.

The provision corresponds to President Juncker's political guidelines according to which "*The United States must [...] guarantee that all EU citizens have the right to enforce data protection rights in U.S. courts, whether or not they reside on U.S. soil*. *Removing such a discrimination will be essential for restoring trust in transatlantic relations*". Likewise, it responds to the European Parliament Resolution of 12 March 2014 on the U.S. NSA

[9] A "Covered Country" pursuant to the U.S. Judicial Redress Act is a country i) that has concluded with the U.S. an agreement which provides for appropriate privacy protections for information shared for law enforcement purposes (or which has effectively shared information for law enforcement purposes and has appropriate privacy protections for such shared information); ii) that permits the transfer of personal data for commercial purposes through an agreement with the U.S. or otherwise; iii) whose policies regarding the transfer of personal data for commercial purposes do not materially impede the national security interests of the United States. The designation of a country as "covered country" is carried out by the U.S. Attorney General.

surveillance programme, by which the Parliament asked to immediately resume the negotiations with the U.S. on the "Umbrella Agreement" to "*put rights for EU citizens on an equal footing with rights for US citizens (…)*" and to provide "*effective and enforceable (…) judicial remedies for all EU citizens in the US without any discrimination*".[10]

Paragraph 3 of Article 19 clarifies that the extension of the three above-mentioned judicial redress grounds is without prejudice to other judicial redress avenues that are otherwise available with respect to data processing (e.g. under the Administrative Procedure Act, the Electronics Communication Privacy Act or the Freedom of Information Act). These other legal bases for judicial redress are open to all EU data subjects concerned by the data transfer for law enforcement purposes, regardless of their nationality or place of residence.

(iv) Aspects relating to the application of the Umbrella Agreement and oversight

(i) Accountability (Article 14)

Measures shall be in place to promote accountability of the authorities processing personal data covered by the Umbrella Agreement. In particular, when personal data is further shared by the receiving authority with other authorities, the latter should be notified of the safeguards applicable under this Agreement as well as possible additional (restrictive) conditions that have been attached to the transfer pursuant to Article 6(3) (on purpose and use limitations). Serious misconduct shall be addressed through appropriate and dissuasive criminal, civil or administrative sanctions.

Measures to promote accountability also include, as appropriate, discontinuation of further transfers of personal data to entities of the Parties not covered by the Umbrella Agreement, in case they do not ensure an effective protection of personal information in light of the purpose of the Agreement (and in particular of the purpose limitation and onward transfer provisions). This provision addresses the situation where personal data is sent by an EU authority to a U.S. federal authority (*i.e.* an authority covered by this Agreement) and then further transferred to a law enforcement authority at State level. Under its constitutional rules, the U.S. is limited in its capacity to bind its federated States at international level.[11] Yet, to ensure continuity of protection to the data transferred to U.S. federal agencies and then shared with law enforcement agencies at State level, this Article (i) includes in its scope the "other authorities" of the Parties (*i.e.* the authorities not covered by this Agreement such as U.S. States' authorities); (ii) stipulates that the safeguards provided under the Umbrella Agreement be notified to them; and (iii) provides that, as appropriate, transfers to such authorities be discontinued in case they do not effectively protect personal data in light of the purpose of the Umbrella Agreement and in particular of its articles on purpose limitation and onward transfers.

By aiming at ensuring that the competent law enforcement authorities will be held accountable for compliance with the Umbrella Agreement, this Article is an important building block of an effective system of enforcement and oversight under the Agreement. It

[10] See § 57 and point BJ of the Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, (2013/2188(INI), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//EN

[11] Being a federal republic, there is a division of powers between the federal government and the government of the individual States (see also Article 5 (2) of the Umbrella Agreement in this respect).

will also facilitate the introduction of claims by individuals in cases of misconduct (and consequent liability of public authorities).

Finally, EU authorities will be able to raise concerns with and receive relevant information from their U.S. counterparts on how they comply with their obligations under Article 14 (including on the measures taken in this respect). Also, in the context of the joint reviews (see *infra* Art. 23), particular attention will be paid to the effective implementation of this Article.

(ii) Effective oversight (Article 21)

The Parties shall have in place one or more public authorities exercising independent oversight functions and powers, including review, investigation and intervention. These authorities shall have the power to accept and act upon complaints made by individuals relating to the measures implementing the Umbrella Agreement and refer violations of law related to this Agreement for prosecution or disciplinary action. Taking into account the particularities of the U.S. system, a combination of supervisory authorities (including Chief Privacy Officers, Inspector Generals, the Privacy and Civil Liberties Oversight Board etc.) will cumulatively exercise the oversight functions that data protection authorities carry out in the EU.

This article complements the safeguards available on the basis of the access, rectification and administrative redress provisions. In particular, it allows individuals to lodge complaints before independent authorities about how the other Party has implemented the Umbrella Agreement.

(iii) Cooperation between oversight authorities (Article 22)

Oversight authorities will cooperate with a view to ensuring effective implementation of the Agreement and in particular as regards the system of indirect exercise of individual rights to access, rectification and administrative redress (see *supra* Art. 16-18).

Moreover, national contact points shall be established to assist with the identification of the oversight authority to be addressed in a particular case. Given in particular the existence of a number of different oversight authorities in the U.S., the creation of a central "entry point" for requests of assistance and cooperation is designed to contribute to an efficient handling of these requests.

(iv) Joint Review (Article 23)

The Parties will conduct periodic joint reviews of the implementation and effectiveness of the Umbrella Agreement, placing particular attention on the effective implementation of the articles concerning individual rights (access, rectification, administrative and judicial redress), as well as the issue of transfers to territorial entities not covered by the Agreement (*i.e.* U.S. States). The first joint review will be conducted no later than three years from the entry into force of the Agreement and thereafter on a regular basis.

The composition of the respective delegations shall include representatives of both data protection authorities and law enforcement/justice authorities, the findings of the joint reviews will be made public.

(v) Final Provisions

The Umbrella Agreement contains a number of final clauses regarding:

- the notification to the other Party of any acts that materially affect the implementation of the Agreement. The U.S. will specifically notify the EU of any measure relating to the application of the provisions of the Judicial Redress Act (Article 24);
- consultations in case there are disputes regarding the way the Agreement is interpreted or applied (Article 25);
- the possibility to suspend the Agreement by one Party in case of material breach of the Agreement by the other Party (Article 26);
- the territorial application of the Agreement in order to take into account the specific situation of the United Kingdom, Ireland and Denmark (Article 27);
- the unlimited duration of the Agreement (which is justified by the nature of the Agreement as a framework providing for protections and safeguards, as well as in the light of the possibility to suspend and terminate the agreement) (Article 28);
- the possibility for each Party to terminate the Agreement by notification to the other Party, while it is specified that personal information transferred prior to the termination will continue to be processed in accordance with the rules of the Umbrella Agreement (Article 29, par. 2 and 3);
- the entry into force of the Agreement the first day of the month following the date in which the Parties have exchanged notifications indicating completion of their internal approval procedures (Article 29, par. 1);
- the language clause (immediately preceding the signature line) providing that (i) the Agreement will be signed in English and drawn up by the EU in the other 23 EU official languages; (ii) the possibility after the signature to authenticate the text of the Agreement in any of these other EU official languages by means of an exchange of diplomatic notes with the U.S.; (iii) in case of divergence between different authentic language versions of the Agreement, the English version will prevail.

2016/0126 (NLE)

Proposal for a

COUNCIL DECISION

on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 in conjunction with Article 218 (6)(a) thereof,

Having regard to the proposal from the European Commission,

Having regard to the consent of the European Parliament,[12]

After consultation of the European Data Protection Supervisor,

Whereas:

(1) In accordance with Council Decision […] of […][13] the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses (the "Agreement") was signed on XX XXXX 2016, subject to its conclusion at a later date.

(2) The Agreement aims at establishing a comprehensive framework of data protection principles and safeguards when personal information is transferred for criminal law enforcement purposes between the U.S., on the one hand, and the EU or its Member States on the other. The objective is to ensure a high level of data protection and, thereby, enhance cooperation between the parties. Whilst not being itself the legal basis for any transfer of personal information to the U.S., the Umbrella Agreement supplements, where necessary, data protection safeguards in existing and future data transfer agreements or national provisions authorising such transfers.

(3) The Union has competence covering all the provisions of the Agreement. In particular, the Union has adopted Directive 2016/XXX/EU[14] on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

(4) The European Union has exclusive competence to the extent that the Agreement may affect common Union rules or alter their scope.

---

12 Consent of [date], OJ C[…], […], p. […].

13 OJ …

14 Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, repealing Council Framework Decision 2008/977/JHA.

(5) In accordance with Article 6a of the Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, the United Kingdom and Ireland are not bound by the rules laid down in the Agreement which relate to the processing of personal data when carrying out activities which fall within the scope of Chapter 4 (Judicial cooperation in criminal matters) or Chapter 5 (Police cooperation) of Title V of Part Three of the TFEU where the United Kingdom and Ireland are not bound by the rules which require compliance with the Agreement.

(6) In accordance with Articles 1 and 2 of Protocol 22 on the Position of Denmark annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Decision and is not bound by the Agreement or subject to its application.

(7) The Agreement should be approved on behalf of the Union,

HAS ADOPTED THIS DECISION:

Article 1

The Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses is hereby approved on behalf of the European Union.

The text of the Agreement is attached to this Decision.

Article 2

The President of the Council shall designate the person empowered to proceed, on behalf of the Union, to give the notification provided for in Article 29(1) of the Agreement, in order to express the consent of the European Union to be bound by the Agreement.

Article 3

This Decision shall enter into force on the day of its publication in the *Official Journal of the European Union*.[15]

Done at Brussels,

For the Council
The President

[15] The date of entry into force of the Agreement for the European Union will be published in the *Official Journal of the European Union* by the General Secretariat of the Council.