COUNCIL OF THE EUROPEAN UNION

Brussels, 9 April 2014

8761/14

RESTREINT UE/EU RESTRICTED

JAI 220
USA 9
DATAPROTECT 56
RELEX 319

NOTE

from :	Commission Services
to :	JHA Counsellors
No. prev. doc. :	5999/12 JAI 53 USA 2 DATAPROTECT 13 RELEX 76 17480/10 JAI 1049 USA 127 DATAPROTECT 98 RELEX 1069 RESTREINT UE
Subject :	EU-US data protection "Umbrella Agreement" - Commission Services Non-Paper on state of play of negotiations

Delegations will find in Annex Commission Services Non-Paper on state of play of negotiations on EU-US data protection "Umbrella Agreement".

ANNEX

EU-US DATA PROTECTION "UMBRELLA AGREEMENT"

NON-PAPER ON STATE OF PLAY OF NEGOTIATIONS

1. INTRODUCTION

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 on the protection of personal data when transferred and processed for purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters ("umbrella agreement"). Detailed "Negotiating Directives" are annexed to the decision.

On 28 March 2011, the Commission opened negotiations with the US side.

The purpose of these negotiations is to agree on a comprehensive framework of data protection principles and safeguards, ensuring a high level of protection, that will apply to all data transfers taking place in the context of transatlantic police and judicial co-operation in criminal matters.

In accordance with Article 2 of the Council decision authorising the opening of negotiations, the Commission has reported after each negotiating session to the designated special committee (JHA Counsellors) on the progress of the negotiations. In accordance with Article 218(10) TFEU, the European Parliament has likewise being immediately and fully informed, in the framework of its Committee for Civil Liberties, Justice and Home Affairs (LIBE). On 3 February 2012, the Commission services also shared with the Council's special committee and the LIBE committee a non-paper providing a state of play of the negotiations.

In light of the progress achieved in these negotiations, the Commission services consider it appropriate to provide a written overview of the issues on which a common understanding has emerged so far. The present non-paper serves this purpose.

The two sides have reached to date a common understanding on a substantial number of issues covering a large part of the future articles of the agreement.

The issues on which provisional agreement has been reached can be grouped as follows: (i) scope and purpose of the agreement; (ii) substantive principles and (iii) enforcement and oversight mechanisms. These agreed principles are being currently translated into legal texts, with the proviso **that nothing is agreed before everything is agreed**. Work has also started on the definitions and final provisions.

This non-paper does not tackle the question of avenues of judicial redress for EU citizens when their data is shared with the US for law enforcement purposes as a satisfactory solution has not yet been found on this point. The importance of this issue was re-stated in the Commission's Communication "Rebuilding Trust in EU-US Data Flows" of 27 November 2013. The Commission has made clear to the US that the creation of such rights either in the Agreement or in self-standing legislation is a key component of a deal. This was reflected in the EU-US Summit Joint Statement of 26 March 2014 which states that: "We reaffirm our commitment in these negotiations to work to resolve the remaining issues, including judicial redress."

2. SCOPE AND PURPOSE OF THE AGREEMENT

This first group of issues relates to the function of the future umbrella agreement and the delineation of its contours, thereby framing the situations in which data transfers for criminal law enforcement purposes can legitimately take place between the EU and the US.

2.1. Purpose

The two sides agree that:

- the purpose of the agreement is to **ensure a high level of protection of personal information** and to enhance cooperation between the US and the EU for the prevention, investigation, detection or prosecution of criminal offences. Ensuring a high level of protection will, therefore, appear as a first and "self-standing" purpose of the agreement;

- the purpose of the agreement shall cover and be limited to **the prevention, detection, investigation and prosecution of criminal offences, including terrorism**;

- the umbrella agreement will establish the framework for the protection of personal information transferred between the Parties, but it will **not in itself be the legal basis** for any transfers of personal information and **a legal basis for such data transfers will always be required.** This means that for a data transfer to take place it will always have to be based on a specific agreement or domestic law concretizing the protections and safeguards laid down in the umbrella.

These agreed principles reflect the requirements of the Negotiating Directives, in particular Directives n. 1 ("The purpose of the Agreement shall be to ensure a high level of protection of fundamental rights and freedoms of individuals and in particular the right to privacy (…) when personal data are transferred and processed (…) for the purpose of preventing, investigating, detecting or prosecuting crime, including terrorism, in the framework of police and judicial cooperation in criminal matters…") and 6 ("The Agreement shall explicitly state that cannot be the legal basis for any transfers of personal data, including from private entities, between the European Union and the US and that a specific legal basis for such data transfers shall always be required").

2.2. Scope

The two sides agree that:

- in line with the agreement reached on purpose, the umbrella agreement will cover personal data transferred for purposes of **prevention, investigation, detection or prosecution of criminal offences**;

- this will include **both** transfers between competent criminal law enforcement authorities of the Parties and transfers taking place pursuant to an agreement between the Parties. Agreements providing that private companies may transfer data to a law enforcement authority of the other Party (such as under PNR or TFTP) will therefore fall within the scope of the umbrella agreement;

- the agreement will be without prejudice to transfers or other forms of cooperation between US and Member State's competent authorities responsible for safeguarding **national security**.

This is in line with the requirements of the Negotiating Directives. Directives n. 4 and 7 require that the agreement apply to all data transfers between the EU and the US "for the purpose of preventing, investigating, detecting or prosecuting criminal offences in the framework of police cooperation and judicial cooperation in criminal matters", including data obtained from private companies in case a law enforcement authority has been authorised by the other Party to receive such data directly from private companies. Directive n. 12 specifies that the agreement shall be without prejudice to the activities in the field of national security.

A purpose and scope defined in the above-mentioned terms will ensure that the protections and safeguards provided by the umbrella agreement will apply horizontally to the whole area of transatlantic law enforcement co-operation in criminal matters. This represents a significant improvement compared to the present situation which is characterised by fragmented, non-harmonised and often weak data protection rules, found in a patchwork of multilateral, bilateral and sectoral instrument. Having a framework agreement of general scope will also facilitate the negotiation and conclusion of future specific data sharing agreements on the basis of an already agreed set of data protection rules.

3. SUBSTANTIVE PRINCIPLES

These principles include a number of safeguards that relate directly to the level of protection afforded to data subjects and the rights of which they can avail themselves, as well as obligations addressed primarily to law enforcement authorities. The latter can also be beneficial for data subjects, as they clarify the obligations to which these authorities are subject and contribute to creating the conditions for the exercise of individual rights.

3.1. Retention period

The two sides agree that:

- processing of data in each Party will be subject to **specific retention periods** in order to ensure that the data will **not be retained for longer than necessary and appropriate**;
- to be deemed appropriate, the duration of these retention periods will have to take into account a **number of elements, in particular the purposes of processing or use, the nature of the data and the impact on the rights and interests of the affected persons**;
- where the Parties conclude an agreement on the transfer of "programme-based" (bulk) data, the **agreement will contain a specific and mutually agreed upon provision on retention period**;
- retention periods will have to be **published or otherwise made publicly available**.

This reflects the requirement laid down in Negotiating Directive n. 8(e) in relation to erasure of data that the Agreement shall provide for "an obligation to set appropriate time limits for erasure - the exact period of which is to be specified in specific agreements or otherwise".

The setting of an obligation to provide for specific and appropriate retention periods goes beyond what is found in most existing agreements and can thereby bring significant added value compared to the current situation. Furthermore, the agreement reached as regards "programme-based" exchanges of data constitutes an important guarantee: it ensures that any future agreement on bulk transfers of "ordinary people" data will have to contain a provision setting a precise retention period that will thus need to be negotiated and agreed between the parties to that agreement (while the principle that such agreements shall contain a specific retention period is accepted and will not have to be negotiated again). Finally, the obligation to publish or make otherwise publicly available applicable retention period is an important element of transparency.

3.2. Onward transfer

The two sides agree that:

- any onward transfer to a third State or an international organisation of data relating to a specific case will be subject to the **prior consent of the competent authority which has originally sent the data**;

- when deciding to grant its consent, the originally sending 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 State or international organisation offers an appropriate level of protection of personal data**;

- as regards onward sharing of "programme-based" data (e.g. further transfer of data extracted from schemes such as PNR), it may only take place in accordance with **specific conditions set forth in an agreement between the Parties and providing due justification for the onward transfer**;

- this agreement shall also provide for **appropriate information mechanisms between competent authorities** on the onward transfer.

These agreed principles follow the requirements set forth in Negotiating Directives n. 8(o) and (p), in particular by making the prior consent of the original sending competent authority the main condition for the onward transfer. This means that in case a US authority intends to further transfer data it has received from the EU to a third country/international organisation, it will have first to obtain the consent of the law enforcement authority in the EU which has originally transferred the data to the US. Furthermore, as for retention periods, the outcome of the negotiations takes expressly into account the special sensitivity of bulk exchanges of "ordinary people" data in that it requires that any further transfer of such data may only take place under specific conditions that have to be duly justified as well as agreed between the Parties.

3.3. Non-discrimination

The two sides are working on a non-discrimination clause that should guarantee that the Parties will **apply the provisions of the umbrella agreement without discrimination between their own nationals and residents and those of the other Party**.

Such a provision has the potential to complement or even strengthen other provisions of the future agreement (in particular those providing safeguards to individuals) by contributing to ensure that Europeans will benefit from equal treatment with US citizens when it comes to the implementation of the agreed provisions by US authorities. The yet unresolved issue of judicial redress (in particular, the availability of judicial redress to Europeans who are not resident in the US) may also benefit from an agreement on a non-discrimination provision.

3.5. Automated decision-making

There is a common understanding that decisions negatively affecting the relevant interests of an individual **cannot be based solely on 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.

Although the Negotiating Directive do not specifically address this issue, it was considered important to include such a provision in the future umbrella agreement. The agreed principle means that data processing that may result, in the context of e.g. profiling, in decisions producing adverse actions concerning the relevant interests of an individual cannot take place unless authorised by law and subject to appropriate safeguards. It is based on a similar principle agreed in the framework of the EU-US High Level Contact Group (HLCG) and goes beyond existing US-Member States bilateral agreements which do not generally cover automated decision making as such.

3.6. Notification of a data breach incident

There is a common understanding that in case of a security incident in which there is a significant risk of damage (unauthorised access or disclosure, accidental loss or destruction etc.):

- appropriate action shall **be promptly taken to mitigate the damage**;
- on this basis, the **incident would, in principle, be notified to both the provider of the data** (i.e. the law enforcement authority of the other party) **and, where appropriate given the circumstances of the incident, the individual concerned;**
- **exceptions to the notification obligation will be exhaustively listed** in the provision and correspond to reasonable limitations (e.g. national security, ongoing criminal investigation etc.).

By laying down a general notification obligation in cases of a data breach, these agreed principles are in line with the requirements of Negotiating Directive 8(g). They also go beyond existing US-Member States and US-EU agreements that do not address at all this issue or contain less affirmative wording. It is also worth noting that there was no corresponding HLGC principle on data breach notification.

3.7. Data quality and integrity

The two sides agree that:

- they shall take reasonable steps to ensure that personal data is maintained with **accuracy, relevance, timeliness and completeness for lawful processing of the information**;
- for this purpose, they shall have in place **procedures to ensure the quality and integrity** of personal data;
- where the recipient/provider of the information becomes aware of significant doubts as to the relevance, timeliness, completeness or accuracy of the transferred personal data, it shall, where feasible, advise the provider/recipient.

This reflects Negotiating Directive 8(c) that requires the data to be processed fairly and lawfully, be accurate and, where necessary, be kept up to date. The explicit understanding between the parties that the personal data should not only be accurate but also relevant, timely and complete guarantees data quality to a greater extent than most of the EU-Member States existing agreements. This also is more beneficial to EU data subjects than certain EU-US sectoral agreements which are silent on this issue.

3.8. Data security

The two sides have a common understanding that:

- **appropriate technical, security and organisational arrangements are to be put in place for the protection of personal information against accidental loss, accidental or unlawful destruction or unauthorised disclosure, access or use**;

- such arrangement shall also include appropriate safeguards regarding the **access to personal data only by authorised staff**.

Read together with the common understanding reached in relation to data breach notification (see 3.6.), this agreed principle contributes to ensuring a high level of protection of the security of personal data. It expands the requirements set forth negotiating Directive n. 8 (h). Compared to similar provisions in existing EU-US/Member States-US agreements, it extends and generalises data security safeguards at horizontal level, bringing thus concrete benefits to EU data subjects.

3.9. Transparency

There is a common understanding that individuals are entitled to receive information (though general or individual notices and with some restrictions) regarding the **purposes 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**.

Reflecting Negotiating Directive n. 8(m), these transparency obligations go beyond most existing agreements that either rely entirely on what is provided for under the applicable national law or contain less explicit and comprehensive language in terms of the individual's right to be informed. By raising the individuals' awareness on why and by whom their data is processed, it also concretely contributes to the possibility for individuals to exercise their rights to access, rectification or redress (see 4.1. and 4.2.).

3.10. Maintaining records

The two sides are in agreement that they shall have in place **effective methods (such as logs) of demonstrating the lawfulness of processing and use of personal information**.

In line with Negotiating Directive n. 8(i), this requirement represents an important safeguard for individuals as it puts an onus on law enforcement authorities to be able to demonstrate that a particular processing operation was carried out in accordance with the law. The obligation to document data processing operation entails, in particular, that there will be a "trace" in case of unlawful processing. This could facilitate the handling of complaints and the introductions of claims regarding the lawfulness of the processing.

4. ENFORCEMENT AND OVERSIGHT MECHANISMS

4.1. Access and rectification

As regards access, the two sides agree that:

- any individual will be entitled to **obtain access to his or her personal data**;
- the **grounds for restricting access will be set out exhaustively in the relevant provisions of the umbrella agreement** and correspond to reasonable limitations (e.g. safeguarding national security, protection of law enforcement sensitive information, avoid obstructing pending investigations or prejudicing investigation or prosecution of criminal offenses, projection of rights and freedoms of others)

- an individual is entitled to **authorise, where permitted by domestic law, an oversight authority (i.e. a Data protection Authority for a EU data subject) to request access on his or her behalf;**

- if access is denied or restricted, the requested authority shall provide the individual (or his or her duly authorize representative) a response setting forth **the reasons for the denial or restriction of access**.

Concerning rectification, both sides are in agreement that:

- any individual will be entitled to **seek correction or rectification of his or her personal data in case it is either inaccurate or it has been improperly processed**;

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

- an individual is entitled to **authorise, where permitted under domestic law, an oversight authority (i.e. a Data Protection Authority for a EU data subject) or another representative to seek correction or rectification on his or her behalf;**

- if correction or rectification is denied or restricted, the requested authority shall provide the individual (or his or her duly authorised representative) a response setting forth the **reasons for the denial or restriction of correction or rectification**.

The common understanding reached on access and rectification reflects the requirements laid down in Negotiating Directives n. 8(k) and (g) as regards both the exercise of the rights to access and rectification and the limitations to which these rights may be subject. In addition, it is foreseen that individuals will also be able to channel their requests for access/rectification through an oversight authority. By ensuring that they can request access or rectification through an authority and a legal system they are familiar with, such a system of indirect exercise of rights should concretely assist the data subjects when seeking to enforce their rights. This series of agreed principles represents a significant improvement compared to the present situation as individuals do not enjoy such specific and detailed safeguards under existing EU/Member States-US agreements.

4.2. Administrative redress

The two sides have agreed that, should **an individual disagree with the outcome of his or her request for access/rectification or in case of improper processing of personal data**, he or she will be entitled to:

- **seek administrative redress;**
- **authorise, where permitted under applicable domestic law, an oversight authority (i.e. a DPA for a EU data subject) or another representative to seek administrative redress on his or her behalf;**
- obtain from the authority from which relief is sought **a written response, including, where applicable, the ameliorative or corrective actions taken**.

This is line with the Negotiating Directives n. 8 (k) and (n) which require that any person whose data are processed under the agreement has a right, in case of disagreement, to refer the matter to an independent public authority. As for access and rectification, the possibility of an indirect exercise of this right is foreseen in order to facilitate its effective enforcement.

The agreement reached on access, rectification and administrative redress is of particular relevance for the protection of EU data subjects: they will be able, for the first time, to avail themselves of rights of general application for any transatlantic transfer of data in the criminal law enforcement sector.

4.3. Effective Oversight

The two sides agree that:

- **the Parties shall have in place public authorities exercising independent oversight functions and powers, including investigation, intervention and review**;

- these authorities shall have the power, *inter alia*, to accept and **act upon complaints made by individuals relating to the measures implementing the umbrella agreement**.

It was also agreed, in accordance with the relevant HLCG principle and taking into account the particularities of the US system, that 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. These authorities and their powers will be clarified in an exchange of explanatory letters separately from but prior to the conclusion of the agreement.

The common understanding on an effective oversight system reflects the requirements laid down in Negotiating Directive n. 9 and complements the safeguards available on the basis of the access, rectification and administrative redress provisions. It will bring significant added value as the existing bilateral agreements between the US and Member States generally refer to a mere "verification procedure", typically performed by the authorities exchanging the data and not involving an independently acting oversight authority. It generalises and expands to the whole law enforcement sector the principle of independent oversight (which is not present as such in most existing agreements) as a core data protection requirement.

4.4. Accountability

Both sides agree that:

- measures shall **be in place to promote accountability by competent authorities;**
- this shall include **appropriate and dissuasive criminal or administrative sanctions** in case of serious misconduct.

This common understanding is in line with negotiating Directive n. 8(q) which requires that public officials or authorities be held liable for non-compliance with the agreement, including through effective and dissuasive sanctions. It will bring significant added value, as it goes beyond most of the existing agreements with the US, which do not contain provisions on accountability. By aiming at ensuring that the competent law enforcement authorities will be accountable for compliance with the future umbrella agreement, it is an important building block of an effective system of enforcement and oversight under this agreement. It will also facilitate the introduction of claims by individuals as to the liability of public authorities in cases of misconduct under this agreement.

4.5. Cooperation between oversight authorities

The two sides agree that:

- **consultations between authorities conducting oversight shall take place with respect to carrying out the functions in relation to this agreement, in particular with a view towards ensuring effective implementation of the articles on access, rectification and administrative redress**;
- **national contact points** shall be established to assist with the identification of the oversight to be addressed in a particular case.

In line with Negotiating Directive n. 11, the common understanding on cooperation between oversight authorities aims at facilitating the effective implementation of the Agreement, in particular as regards the system of indirect exercise of individual rights. Moreover, national contact points – similar to those foreseen in a number of law enforcement cooperation agreements – will be established in order to assist with the identification of the competent oversight authority in a particular case. Given in particular the number of different oversight authorities in the US, the creation of a central "entry point" for requests of assistance and cooperation should contribute to a smooth handling of these requests. This brings clear added value compared to the current situation as most of the existing agreements has language cooperation between oversight authorities.

5. CONCLUSION

Following the revelations on US large-scale surveillance programmes, both the Commission in its Communication on "Rebuilding Trust in EU-US Data Flows" of 27 November 2013 and the European Parliament in its resolution adopted on 12 March 2014 on the impact of the surveillance programmes on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs area have identified the conclusion of an umbrella agreement, ensuring a high level of protection of personal data, as an essential element for rebuilding confidence in transatlantic data exchanges.

While common understanding has now been reached between the two sides on most of the issues covered by the Negotiating Directives, the remaining areas of discussion concern issues which are key to a successful conclusion of these negotiations. This includes the provisions on judicial redress, purpose limitation and sensitive data. The upcoming negotiation rounds will focus on these issues.

The Commission services will continue to keep the Council and the Parliament fully informed of all relevant developments in these negotiations.