Brussels, 19 November 2010
D(2010) 837566

Vice-President Viviane Reding
Commissioner for Justice, Fundamental Rights and Citizenship
European Commission
Rue de la Loi, 200
B - 1049 BRUSSELS

Subject: EU-US General Agreement

Dear Vice President,

On 26 May 2010 the European Commission presented the draft negotiating mandate for 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 (hereafter: the EU-US general agreement). The Article 29 Working Party understands the negotiating mandate has been under discussion in both the Council and the European Parliament in recent months and may be adopted by the Justice and Home Affairs Council in early December.

The Working Party regrets that it has not been consulted on the content of the negotiating mandate for this agreement, since these negotiations with the US are bound to be one of the most important steps within the area of data protection the EU is to take in the coming years. The Working Party has therefore decided, having in mind their joint contribution with the Working Party on Police and Justice (WPPJ) to the public consultation on the EU-US agreement[1], to address this letter to the three main EU institutions to voice its concerns.

Since the draft mandate as adopted by the European Commission is confidential, the Working Party has had to base its considerations on publicly available information. You will find that the issues raised in this letter are consistent with the joint contribution mentioned above, as well as with the recently adopted opinion on the Communication on a Global Approach for the transfer of Passenger Name Record (PNR) data[2]. Nevertheless, the European Data Protection Authorities feel it is necessary to reiterate these points as the future EU-US general agreement will set the standard for many years to come, including for negotiations on similar agreements with other third countries.

[1] Joint Contribution of the European Data Protection Authorities as represented in the Working Party on Police and Justice and the Article 29 Working Party
[2] Opinion 7/2010 of 12 November 2010

Scope of the agreement

The future EU-US general agreement is to be seen as a so-called 'umbrella agreement', in which detailed data protection provisions are to be established. The agreement is however a *lex generalis* and cannot be considered a legal basis for data sharing. This means that for specific exchanges of personal data from the EU to the US and vice versa, specific sectoral agreements remain necessary. In these sectoral agreements, a standard provision referring to the EU-US general agreement should be included. Since the purpose of the EU-US general agreement is to ensure a coherent approach and equal treatment of citizens on all occasions, it should not be possible to derogate from that agreement in a specific sectoral agreement. Existing sectoral agreements should until their revision be applied consistently with the data protection provisions of the EU-US general agreement.

One of the main questions to be discussed with the US concerns the scope of the agreement. The Working Party remains in favour of a widely applicable agreement, to ensure a coherent and high level of data protection. That said, the Working Party argues at the same time for a clear purpose limitation. This means the agreement should be applicable to all transfers of personal data to prevent, detect, investigate and prosecute serious transnational crime and terrorist acts. This purpose should be clearly defined by the agreement, preferably including a definition of 'law enforcement purposes'.

The Working Party is hesitant about the inclusion of data related to immigration, visa and asylum. These data are not to be used for law enforcement purposes, since that would be contradictory to the purpose limitation principle. However, if these data are in the future exchanged with the US for law enforcement purposes based on specific agreements approved by the EU Member States and the European Parliament, the data protection principles of the EU-US general agreement should be applicable in full. If that were to be the case, only personal data could be exchanged which is held in police databases and lawfully used for law enforcement purposes in the first place. Civil law data should not be included in the agreement, as it is of a completely different nature.

National security exception

From a non-final version of the draft mandate, the Working Party understands the Commission is considering including an exception in the agreement for the transfer of data concerning 'essential national security interests and specific intelligence activities in the field of national security'. The Working Party understands this is due to the fact that national security remains an exclusive domain for the Member States, but nevertheless opposes this exception. As mentioned before, the future EU-US agreement should also cover bilateral agreements between Member States and the US, at which level agreements dealing with national security could be negotiated.

One of the main purposes of the future agreement is to offer a high level of data protection for data exchanged for, among others, the purpose of fighting terrorism. Therefore, it is fundamental that data used in the fight against terrorism is not immediately identified as essential to national security interests and so not covered by the agreement. If any exception with regard to the protection of information of relevance to, or stemming from, the security services is to be included in the agreement - of which the European data protection authorities are not convinced - it should be formulated very specifically, to make sure the exception can only be invoked under very specific circumstances.

Information from private entities
Information that is to be used in transatlantic police and judicial cooperation in criminal matters will mainly originate from European law enforcement authorities. However, the amount of data requested from private entities to fight crime is ever growing. The most clear example is the TFTP II agreement giving the US Treasury the possibility to request information related to bank transfers from the EU. Preparations for a new PNR agreement are also being made at this time. The Working Party therefore believes that information originating from private entities which is requested by the US competent authorities to prevent, detect, investigate and prosecute transnational crime and terrorist acts should in any case be covered by the future general EU-US agreement.

Application of the EU-US general agreement to existing agreements
Until now, the US has concluded many bilateral and multilateral agreements with the Member States and the EU to exchange personal data for police and criminal justice cooperation. These agreements may have separate data protection regimes and therefore different and not always consistent levels of protection for individuals. It would therefore be advantageous if all these regimes were replaced by a single, uniform and consistent data protection regime. However, at a hearing in the European Parliament on 25 October 2010, US ambassador Kennard stated the US is concerned about the so-called 'retroactive' application of the future agreement. This would 'sow confusion among law enforcement and judicial authorities and threaten our most serious prosecutions', he said. According to the Working Party it is rather the current situation that sows confusion, both for the citizen wishing to exercise his or her rights and for the supervisory authorities wishing to exercise theirs. The Working Party therefore urges the Commission as the designated negotiator for the EU to make sure the future agreement will be 'retroactively' applicable and thus cover all existing multilateral and bilateral agreements between the EU and/or its Member States and the US, unless the current level of data protection is higher than the level of protection offered by the EU-US general agreement. Where agreements need to be amended to comply with the future EU-US general agreement, a transitional period of no more than three years would be acceptable.

In this connection, the Member States should provide the Commission with copies (or a list) of the existing bilateral and multilateral agreements they entered into with the US insofar as they relate to the scope of the future EU-US general agreement.

Respect for fundamental rights
It should speak for itself that the future agreement should fully meet the conditions set out in the EU's legal framework on privacy and data protection, both in the former first and the former third pillars, especially after the entry into force of the Treaty of Lisbon. This means, among others, that the rights attributed to data subjects in both Directive 95/46/EC, Framework Decision 2008/977/JHA and their national implementation should at least be ensured in the agreement. It should speak for itself that all rights attributed to the data subject should be exercisable in practice as well. Specific attention is to be paid to the revision of Directive 95/46/EC which is currently underway, especially since the new comprehensive framework will probably also cover the former third pillar issues. The Working Party considers that even if the revision of the general data protection framework is not concluded before the negotiations on the future EU-US general agreement are finalised, new intra-European developments should be fully taken into account in the negotiations.

Furthermore, the agreement should respect the right of the protection of the citizens' fundamental rights as is laid down in the EU's Charter of Fundamental Rights, which has a

binding legal status since the entry into force of the Treaty of Lisbon. In this regard, one point of specific concern to the European Data Protection Authorities is that data transferred may be used in a way that conflicts with a fundamental right, such as leading to the imposition of the death penalty. The Working Party therefore argues for a provision in the future agreement that denies the transfer of data when these data will be used in a case that may lead to a conflict with the fundamental rights in the Charter.

Data protection principles

The data protection principles that are to be included in the future agreement have mainly been the outcome of the work of the so-called EU-US High Level Contact Group (HLCG). In general, the Working Party recognises that those principles correspond – to a certain extent – to the basic data protection requirements. There are however some principles to which extra attention needs to be paid, mostly following recent experiences with the negotiations resulting in the TFTP II agreement which is unsatisfactory from a data protection perspective. Additionally, the Working Party wishes to stress the importance of state of the art security for all data transfers and data storage, including access logs.

Effective and enforceable rights
First of all, the future agreement should include effective and enforceable rights for all data subjects. The nationality or country of residence of an individual should be of no importance when he or she wants to access, rectify or expunge his or her personal data. Furthermore, enforceable rights go hand in hand with transparency. The authorities receiving and processing data covered by the future agreement, both in the EU and the US, should be as transparent as is reasonably possible in a law enforcement environment. In particular, information should be easily available for individuals on how to exercise their rights, preferably directly but if need be indirectly. If the latter is the case, the agreement should foresee a clear procedure on indirect access and indicate to which public authorities access and rectification requests should be addressed. The Working Party suggests that the European data protection authorities will in that case be designated as the relevant points of contact and will thus receive and process requests of access using their powers and competences and following the procedures foreseen in their national legislation. National data protection authorities should not be seen as a mere ‘mailbox’, as seems to be the case in the TFTP II Agreement. A mechanism for effective cooperation with their data protection ‘counterparts’ in the US should be introduced in the EU-US general agreement.

Administrative and judicial redress
A second point to be explicitly addressed in the agreement is the need for effective judicial redress. It is a fact that the current US Privacy Act of 1974 does not allow for non-US citizens or residents to go to court over a breach of this act. In the Parliaments‘ hearing referred to before, Ambassador Kennard expressed the view that this is not likely to change over the coming years. Therefore, it is of the utmost importance to grant effective redress to individuals by another binding instrument. For this reason it is necessary to include clear and precise procedures in the agreement making it possible for data subjects to seek an effective administrative and subsequent judicial remedy before a competent authority. Once again, no distinction based on the nationality or country of residence of the person(s) involved should be made.

Bulk transfers
Even though this agreement shall not be a legal basis for the transfer of personal data from the EU to the US or vice versa, it should stipulate that any bulk transfer under the conditions of this 'umbrella agreement' is prohibited. All data transfers should at all times be subject to scrutiny on a case-by-case basis, providing for a check of the necessity and proportionality of that specific transfer. The check should also verify whether or not the transfer complies with the principle of purpose limitation.

Onward transfers
The Working Party is concerned about the way the US will handle the personal data received. Strict conditions may apply on the processing of these data, but in the US an independent data protection supervisor to oversee the processing still has not been established. This is one of the main reasons why the Working Party calls for very strict rules on the onward transfer of EU-originating data.

First of all, a distinction should be made between the onward transfer of data to other authorities within the US and transfer to third countries. Where the intra-US transfer is concerned, the Working Party argues for a limited list of clearly defined competent authorities permitted to receive the data to be included as an annex to the future agreement. Transfer of EU-originating data to third countries should in principle not be allowed. Only after ensuring that the onward transfer is authorised on a case-by-case basis by prior express and written approval of the country of origin and while fully respecting the purpose for which the data where transferred to the US in the first place, such a transfer to a third country could be acceptable. Furthermore, the receiving third country should meet the standards that afford an adequate level of data protection, as is meant in article 25 of Directive 95/46/EC and in article 13 of Framework Decision 2008/977/JHA.

In general, it should be pointed out that the authority that has originally requested the data is to be seen as the data controller, who remains responsible for the data even after a transfer to third parties. In case of doubt, the authority concerned should be obliged to withhold its consent to the disclosure of the data to a third party. Also, should misuse be made of the data by such a third party, the data subject should be able to hold the original recipient of the data to account.

Retention periods
As for all data processing, retention periods should be short and at least no longer than necessary for the performance of the defined tasks. In other words, they should be adequate and proportionate. This should be explicitly confirmed in the future agreement, by preference including an absolute maximum retention period. The retention period for a specific situation, depending on the conditions of that data processing defining "no longer than necessary", should subsequently be laid down in the sectoral (multilateral or bilateral) agreements covered by the EU-US general agreement. The sectoral agreement should also include a provision demanding a regular review of the necessity to continue to keep the received data.

Joint review
To guarantee an effective application of the future agreement, it is important that regular joint reviews and evaluations take place. A standard provision to that effect should be included in the future EU-US agreement, as well as in all agreements to be covered by the EU-US general agreement. The Working Party argues for these to be carried out every other year, with the first review to take place 18 months after the entry into force of the future agreement. The

joint review team should contain members from both the EU and the US and include representatives of the European data protection authorities (or of the relevant national data protection authority where bilateral or multilateral agreements without EU involvement are concerned), as is the case for the TFTP II agreement.

Sunset clause
It is necessary to periodically reassess and evaluate the necessity of data exchanges. Such a comprehensive in-depth assessment cannot be done during a review as described above. Therefore a sunset clause which mandates a thorough and independent assessment and evaluation of the provisions of each system for data exchange should be be included in the EU-US general agreement and thus be introduced in every bilateral and multilateral agreement. After the date mentioned in the sunset clause is reached, no data can be exchanged unless the parties to the agreement specifically decide to extend the agreement.

Conclusion

The Working Party welcomes the initiative taken by the Commission to strive for a general agreement with the United States to ensure a high level of data protection when information is exchanged within the cooperation on police and criminal justice matters. Given experiences in the past and recognising the reality that the balance between security and privacy is often not always right, the Working Party is however concerned about the possible outcome of the negotiations. It therefore urges the Commission, the Council and the European Parliament to ensure a strict and far reaching negotiating mandate, to obtain a high level of data protection. Coherence is needed in light of current developments, including the review of the EU data protection legal framework and the proposed negotiations with the US on a new PNR agreement.

As mentioned before, the Working Party recognises the importance of this agreement as one of the most important steps in data protection to be taken in the coming years. The European Data Protection Authorities therefore respectfully request to be given a role in developing the future agreement and to be given regular updates on the state of play. This would enable the Working Party, also given its role as an official advisory body of the Commission on data protection issues, to recommend possible solutions should difficulties arise.

The Working Party looks forward to receiving your response and remains at your disposal for further consultation when clarification or elaboration of its position is required.

Yours sincerely,

On behalf of the Article 29 Working Party,

Jacob Kohnstamm
Chairman of the Article 29
Working Party

Cc: Mrs. Cecilia Malmström, Commissioner for Home Affairs
Mr. Juan Fernando López Aguilar MEP, Chairman of the European Parliaments' Committee on Civil Liberties, Justice and Home Affairs
Mr. Herman van Rompuy, President of the Council of the European Union
Mr. Stefaan de Clerck, Minister for Justice of Belgium