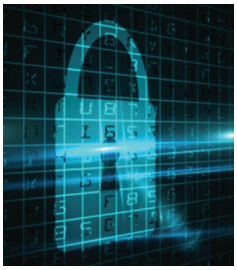
European Commission

FACTSHEET EU-US
NEGOTIATIONS ON DATA PROTECTION

June 2014

What are the EU-US negotiations about?



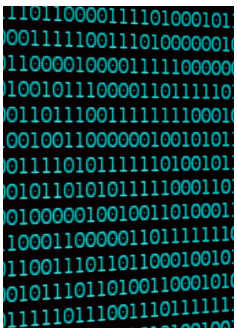
Since **29 March 2011**, the European Union has been negotiating with the United States government an international framework agreement (so-called 'Data Protection Umbrella Agreement') in order to protect personal data transferred between the EU and the U.S. for law enforcement purposes. This includes cases in which personal data is sent from the EU to the U.S. for the prevention, detection, investigation and prosecution of criminal offences, including terrorism.

What is the legal basis and process for the negotiations?

The **Treaty on the Functioning of the EU** (Article 218 of the Treaty on the Functioning of the European Union) sets out the procedure for negotiating and concluding international agreements.

The European Commission is negotiating the data protection framework agreement based on a mandate given unanimously by the Council of the European Union to the European Commission (**Vice-President Viviane Reding**) in December 2010, which authorised the opening of negotiations with the United States (see **IP/10/1661**).

During these negotiations the European Commission keeps the European Parliament fully informed of the discussions with its U.S. counterparts. The European Parliament must approve the negotiated agreement at the end of the process.



When did the negotiations start and how many rounds have there been?

The first round of negotiations took place in March 2011 (see **MEMO/11/203**). So far there have been 20 negotiating sessions, with the most recent one being held on 9-10 June 2014. The European Commission has also reported regularly to EU Member States (at the Justice and Home Affairs Counsellors' meetings and at the Justice Council) on the progress of the negotiations. The European Parliament has likewise been kept fully informed of developments, through its Committee for Civil Liberties, Justice and Home Affairs (LIBE).

What will the Data Protection Umbrella Agreement cover?

The Umbrella agreement will cover all personal data (for example names, addresses, criminal records) transferred from the EU to the U.S., taking place in the context of the prevention, detection, investigation and prosecution of criminal offences, including terrorism. The agreement will put in place a comprehensive framework, ensuring a high level of protection applying to all data transfers taking place in this context.

Justice

What is the added value of the agreement?

1. The agreement will guarantee a high level of protection for EU citizens whose data is transferred to the U.S. (and vice-versa). The agreement does not, in itself, authorise the transfer of data between the EU and the U.S. Its purpose is to complement other agreements signed by the EU or its Member States with the U.S. which enable data transfers by setting out a series of guarantees and safeguards that must always apply. By filling in the gaps, it will bring the level of protection of individuals beyond the currently existing one when data is transferred to the U.S. It will ensure that when personal data is transferred for law enforcement purposes, it is processed with appropriate safeguards for the protection of individuals on both sides of the Atlantic.
2. The agreement can also bring an added value from a law enforcement/police cooperation point of view: future specific data-sharing agreements (such as the Passenger Name Records or the Terrorist Finance Tracking Program today) will be easier and more straightforward to conclude on the basis of the framework provided by the umbrella agreement. In short: The EU can agree to sharing data if we can be sure that personal data transferred is protected and EU citizens have enforceable rights across the Atlantic.

What progress has there been so far?

The negotiations have reached their final stage. The issues on which provisional agreement has been reached include the scope and purpose of the agreement, fundamental principles and oversight mechanisms.

- purpose of the agreement: ensuring a high protection of personal data and improve cooperation between the EU and the U.S. for law enforcement purposes and the prevention of terrorism; the agreement itself does not authorise any data transfers which is why specific data sharing agreements will still be needed in the future.
- Fundamental principles include, for example, non-discrimination and maintaining the quality, integrity and security of data.
- Retention periods: information should not be retained for longer than is necessary and appropriate.
- Right of access and rectification: citizens should be able to access their data – subject to certain conditions – and request that it be corrected if it is inaccurate (for example one's name).
- Effective oversight: oversight authorities need to exercise independent functions and powers, including accepting and acting upon complaints from individuals relating to the agreement and conducting investigations.

What are the outstanding challenges?

A critical outstanding issue which remains is the right of effective judicial redress that should be granted by the U.S. to EU citizens not resident in the U.S. (i.e. ensuring that EU citizens not resident in the U.S. enjoy the same rights as those enjoyed by U.S. nationals in the EU today).

This is significant for two reasons: first ensuring equal treatment, meaning that EU citizens who don't live in the U.S. can obtain the same treatment in terms of judicial redress (meaning they can go to court) as U.S citizens, and secondly ensuring the enforceability of the rights set out in the EU-U.S. agreement. This is an issue which is at the core of the negotiating mandate the Council gave to the Commission. A satisfactory solution is yet to be found on this point. The U.S. recognises how critical this issue is for the EU, and has committed to identifying ways of addressing it, such as through legislative action in Congress. While this commitment from the U.S. side is welcome, a workable legislative solution is yet to be proposed by the U.S.

The importance of equality in judicial redress rights was re-stated in the Commission's Communication **"Rebuilding Trust in EU-U.S. Data Flows"** of 27 November 2013. The importance of addressing this issue was also recognised by the U.S. in a **joint statement made on 18 November 2013** following the EU-U.S. Justice and Home Affairs Ministerial Meeting in Washington. The EU-U.S. Summit **Joint Statement of 26 March 2014** also states that: "We reaffirm our commitment in these negotiations to work to resolve the remaining issues, including judicial redress."

The two sides also still need to come to an agreement regarding the purpose limitation of the data sent to the U.S. The EU seeks to ensure that data shall only be transferred for specified law enforcement purposes, and then processed in a way compatible with these purposes. For instance, the data of a victim of human trafficking cannot be dealt with in the same way as the data of a suspect of human trafficking.

In parallel, negotiations with the U.S. are on-going in order to make the Safe Harbour scheme safer. The European Commission addressed 13 recommendations to the U.S. authorities in November 2013 (see **MEMO/13/1059**). Whereas substantial progress has been achieved on a majority of the recommendations, the U.S. has not yet proposed any solutions regarding the key political issue covered by Recommendation 13, which is limiting access to Safe Harbour data for national security purposes. This is a key issue that will need to be addressed before the Safe Harbour framework can be given a clean bill of health.

Real life example

An EU citizen's name is identical to that of a suspect in a transatlantic criminal investigation. His / her data has been transferred from the EU to the U.S. and accidentally gets collected and included on a U.S. black list. This can lead to a series of consequences from the refusal of an entry visa, to a possible arrest. The EU citizen should be able to have his or her name deleted by the authorities – if necessary by a judge – once the mistake is discovered. Europeans (and Americans) have those rights in the EU. They should have them when their data is exchanged with the U.S. too.

The citizen who believes that his/her data is inaccurate can authorise, where permitted under domestic law, an authority (for instance a Data Protection Authority) or another representative to seek correction or rectification on his or her behalf. If correction or rectification is denied or restricted, the U.S. authority processing the data should provide the individual or the data protection authority acting on his/her behalf with a response explaining the reasons for the denial or restriction of correction or rectification. An individual may also address an oversight authority (a Data Protection Authority for an EU citizen) to seek redress from the U.S. administration on his or her behalf.

Background

Recent speeches by Vice-President Viviane Reding on the EU-US data protection negotiations:

A data protection compact for Europe (January 2014)

Towards a more dynamic transatlantic area of growth and investment (October 2013)

PRISM scandal: The data protection rights of EU citizens (June 2013)