EU/USA Agreement: protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses

2016/0126(NLE) - 29/04/2016 - Preparatory document

PURPOSE: to conclude, on behalf of the European Union, 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.

PROPOSED ACT: Council Decision.

ROLE OF THE EUROPEAN PARLIAMENT: Council may adopt the act only if Parliament has given its consent to the act.

BACKGROUND: in 2006, 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 to explore ways that would enable the EU and the U.S. to work more 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 20091 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.

On 3 December 2010, the Council adopted a decision authorising the Commission to open negotiations on such an agreement between the European Union and the United States of America. On 28 March 2011, the Commission opened negotiations. On 8 September 2015, the Parties initialled the text.

The Agreement should now be concluded on behalf of the European Union.

CONTENT: the Commission proposes that the Council adopt a decision approving, on behalf of the EU, 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 aims to **establish 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 personal data protection when transferred between the U.S., on the one hand, and the EU or its Member States on the other, for law enforcement purposes 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 Agreement **supplements, where necessary, data protection safeguards in existing and future data transfer agreements** or national provisions authorising such transfers.

1) Scope and general objectives: the Agreement aims to establish for the first time, 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 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 adopted on 14 April 2016.

2) Data protection principles and safeguards: the Agreement covers important principles governing personal data processing as well as key safeguards and limitations:

Purpose and use limitations: 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.

The Agreement 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 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.

Onward transfer: if 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 consent** from the law enforcement authority in the EU which has originally transferred the data to the United States. This rule equally applies where 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.

The provisions expressly take 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). The Agreement requires that any further transfer of personal information other than in relation to specific cases, may only take place under **specific conditions** that provide due justification for the onward transfer.

In addition, the Parties to the Agreement must take measures to ensure:

- data **quality a**nd **integrity** of information ;
- information **security** and **notification of an information security incident** ;
- effective methods (such as logs) for demonstrating the **lawfulness of processing** and use of personal information;
- **specific retention periods** in order to ensure that data will not be retained for longer than necessary and appropriate. The retention periods will be subject to periodic reviews and will have to be published or otherwise made publicly available.

Special categories of data: 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).

3) Individual rights: data subjects 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, these being:

- the right to access data and the right to rectification of data which concern them ;
- the right to administrative redress if an individual disagrees with the outcome of his or her request for access/rectification of personal data;
- the right 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

4**) Aspects relating to the application of the Agreement and oversight**: measures must be put in pace in order to:

- promote accountability of the authorities processing personal data covered by the Agreement;
- establish one or more public authorities exercising independent oversight functions and powers, including review, investigation and intervention;
- ensure cooperation between oversight authorities; national contact points shall be established to assist with the identification of the oversight authority to be addressed in a particular case;
- conduct periodic joint reviews of the implementation and effectiveness of the Agreement.

The Agreement will be of **unlimited duration** (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 of suspending and terminating the Agreement).