

Consultation on the future EU-US international agreement on personal data protection and information sharing for law enforcement purposes

All stakeholders and organisations involved in the protection of personal data and/or processing, transfer or sharing of information for law enforcement purposes in the transatlantic context as well as the general public are invited to respond to the public consultation.

In addition to this electronic consultation, the Commission is organising meetings to seek the views of personal data protection authorities of the European Economic Area, European Union Member States' ministries for justice, home affairs as well as law enforcement authorities, and private sector representatives. Moreover, the Commission is keeping fully informed the European Parliament at all stages of the negotiation procedure as stipulated in Article 218 (10) of the Treaty on the Functioning of the European Union. Comments by the aforementioned entities as part of the electronic consultation are also welcome.

Contributions received in reply to the consultation will be published on the internet at the Commission's website. Publication will be regarded as acknowledgement of receipt of your contribution by the Commission.

If you do not wish your contribution to be made public, please indicate this clearly at the beginning of your reply. In that case, your reply will also not be mentioned in future documents that may refer to this consultation.

This document has been prepared by the Commission services for consultation purposes. It does not in any way prejudge, or constitute the announcement of, any position on the part of the Commission on the issues covered.

Background:

Law enforcement agencies on both sides of the Atlantic collect and process personal data in order to prevent, detect and prosecute crime and terrorism. The transfer of personal data is an essential element of transatlantic law enforcement cooperation in order to fight serious transnational crime and terrorism effectively. Consequently the protection of personal data in the context of the processing and transfer of data for law enforcement purposes has been the subject of discussions and negotiations of international agreements between the European Union and the United States of America (US) over the past years.¹

A High Level Contact Group on information sharing and privacy and personal data protection (HLCG) was established by the EU-US Justice and Home Affairs Ministerial Troika on 6 November 2006 to discuss privacy and personal data protection in the context of the exchange of information for law enforcement purposes as part of a wider reflection on how to best prevent and fight terrorism and serious transnational crime. The goal of this group was to explore ways enabling the EU and the US to work more closely together in the exchange of law enforcement information while ensuring that the

¹ US-Europol cooperation agreements:

<http://www.europol.europa.eu/legal/agreements/Agreements/16268-2.pdf>;

<http://www.europol.europa.eu/legal/agreements/Agreements/16268-1.pdf>; US-Eurojust agreement:

http://www.eurojust.europa.eu/official_documents/Agreements/061106_EJ-US_co-operation_agreement.pdf; 2007 Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), OJ L 204 of 4.8.2007, p. 16; 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 purposes of the Terrorist Finance Tracking Programme, OJ L 8 of 13.1.2010, p. 9

protection of personal data and privacy are guaranteed. The HLCG presented a final report on 28 May 2008 and an addendum to this report on 28 October 2009 which identified a set of core privacy and data protection principles and a set of related issues pertinent to the EU-US transatlantic relationship.

The European Council invites the Commission in the Stockholm Programme to propose a recommendation for the negotiation of a data protection and, where necessary, data sharing agreement for law enforcement purposes with the US, building on the work of the HLCG.

The European Data Protection Supervisor presented an opinion on the HLCG 2008 report on 11 November 2008.

This paper non-exhaustively lists questions on which the Commission wishes to seek the opinions of stakeholders with a view to a future EU-US agreement on personal data protection and information sharing for law enforcement purposes.

1. Purpose

What should be the purpose(s) of the agreement? Should the agreement only establish data protection standards for EU-US law enforcement cooperation? Or should it address also wider issues related to the processing and transfer of personal data in the context of transatlantic law enforcement cooperation, e.g. reciprocal information transfer or impact on relations with other third countries?

2. Scope of the agreement

2.1. Material scope

- Should the agreement cover personal data protection when information is transferred that pertains to police cooperation in the area of freedom, security and justice (Title V chapter 5 of the Treaty on the Functioning of the European Union (TFEU))?
- Should it also cover personal data protection when information is transferred in the course of judicial cooperation in criminal matters (Title V chapter 4 TFEU)?
- Should it also be applicable to the transfer of personal data in the context of other Union policies within the area of freedom, justice and security, i.e. the security elements of immigration, visa, asylum and civil law cooperation?

2.2. Personal scope

- Should the agreement only cover government-to-government transfers of information?
- Or should it also be applicable to transatlantic transfers of personal data from private entities to law enforcement authorities? If so, should the conditions on private – public data transfers be in any way different from the government-to-government transfers?

3. Nature of the agreement:

Should the agreement include a provision to the effect that EU and US law enforcement authorities may request from each other the same types/categories of information and personal data (reciprocity)?

4. Data Protection Principles

4.1 Accountability

Should the agreement provide for modalities and consequences of "accountability", e.g. internal and external review procedures? Should the agreement notably provide for a joint review mechanism?

4.2. Individual Access

- Should the agreement spell out the conditions for the right to access one's own personal data?
- If there is no possibility to directly access one's own personal data for justified reasons, should the agreement provide for the possibility of indirect verification through an independent authority responsible for the oversight of the processing in the sending or recipient country?

4.3. Single contact points

- Should the agreement provide for a single contact point in the US in case of data protection concerns related to data transferred from the EU?
- Should the agreement provide for a single contact point in the EU in case of data protection concerns related to data transferred from the US?
- Should the modalities for transparency and assistance to data subjects by US and EU data protection supervisory authorities be spelled out in the agreement?

4.4. Judicial redress

- Should the agreement lay down provisions for effective access to courts for data subjects that believe that their data protection rights have not been respected? How could this be achieved?
- Should laws which discriminate in respect of access to the courts on grounds of nationality or residence be amended?

5. Any other comment

You may introduce here any other comment you would like to make on the future European Union (EU) - United States of America (US) international agreement on personal data protection and information sharing for law enforcement purposes.