European Commission, Directorate-General for Justice, Freedom and Security
Unit A2 – External relations and enlargement
B - 1049 Brussels

Opinion of the Association for Fair Data Processing

This document was elaborated in response to the call for public consultation on the future European Union (EU) - United States of America (US) international agreement on personal data protection and information sharing for law enforcement purposes

Budapest
2010

Introduction

The Association for Fair Data Processing (Tisztességes Adatkezelésért Egyesület in Hungarian) was founded on 6th November 2009 in Budapest, Hungary. This informal association consists of independent scholars, legal and information technology experts. Its aim is to discuss newly emerging problems with respect to personal data protection and freedom of information.

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

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 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 Program 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.

---

[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

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?

The purpose is very definitive: fight against crime, fraud, terrorism – especially of transnational nature – in cooperation with the competent international and national bodies and organizations. The number of the latters are growing, but their efficiency relative to their budget and staff is questionable.

In the EU e.g. Europol, Eurojust, Olaf – just to mention the commonly known international organizations – have been established to serve that purpose based on European treaties, conventions etc., and their activities are regulated under many other legal instruments. In addition both Europol and Eurojust have concluded agreements with the United States of America.

It is also evident, that the key to all that kind of cooperation is the multitude of data gathered on individuals, then processed and exchanged between the organizations concerned. The problem begins with the gathering, because data are gathered on a huge number of persons of which very few might be suspect of crime (see e.g. Passenger Name Record data). An intelligent filtration tool should be developed and used to filter out and erase the data of those who are beyond any suspicion. This notion has been reflected in a document of the Art. 29 WP on "The Future of Privacy"[2].

Within the overall purpose to combat crime the purpose of data protection should be emphasized, so data collected on individuals should meet all the requirements laid dawn by the relevant international and national law and other legally valid instruments.

The debates, reports by the High Level Contact Group on information sharing and privacy and personal data protection, as well as opinions (first of all that of the EDPS) made public in the last few years on international agreements involving transborder flow of personal data prove that people, even members of the European Parliament, are becoming more and more sensitive in that regard. This conclusion is drawn from the fact that the European Parliament recently voted down the SWIFT data sharing agreement with the US, especially for not fully respecting basic data protection principles.

Although the Agreement in force between the United States of America and the European Police Office does not authorize the transmission of data related to an identified or identifiable individuals, it foresees an amendment relating to the exchange of personal data.

---

[2] Article 29 Data Protection Working Party/Working Party on Police and Justice. The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Adopted on 01 December 2009. Chapter 8 Data protection challenges in the field of police and law enforcement

Nevertheless we think any future agreement on law enforcement cooperation – taking into account that not only the word, but also crime are becoming global – either with the US or other third countries should strictly be built on data protection standards (by which, we hope, you understand not only technical standards, but hard law principles, too).

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)?

As we mentioned above the agreement can in the future be amended with certain provisions covering exchange of personal data. Should the US and Europol enter into consultation on that issue, the relevant provisions of TFEU must be considered and scrupulously interpreted. Interpretation is needed because TFEU is very reticent in this regard. According to Art. 88(2)(a):

> "The European Parliament and the Council, by means of regulations adopted in accordance with the ordinary legislative procedure, shall determine Europol's structure, operation, field of action and tasks.
> These tasks may include: the collection, storage, processing, analysis and exchange of information, in particular that forwarded by the authorities of the Member States or third countries or bodies;"

The question is, whether "information" covers personal data or not. Theoretically information is a conclusion drawn from data. Such conclusion e.g. that the person the data of whom were gathered and analyzed might be suspect of crime.

Apart from theory the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters extends the notion of information to cover also personal data, and their exchange with respect to third countries providing for their protection, too.

Therefore it is indispensable that the agreement strictly protects personal data when information is transferred that pertains to police cooperation.

- 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)?

Very naturally yes (see the answer under the previous bullet point).

- 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?

We stand up for any kind of cooperation, when it results in the protection of our fundamental rights. Even if immigration, visa, asylum etc. are not falling under the category of law-enforcement or prosecution of crime, yet immigrants, applicants for visa or asylum might fraudulently use this availabilities to circumvent their detection.

2.2. Personal scope

- Should the agreement only cover government-to-government transfers of information?

Government-to-government transfer is more reliable. Government authorities can make the decision, whether the information kept by them is worth to be transferred. In that regard the national data protection authorities and judicial oversight can play an important role, forming general or specific opinion at the issue.

- 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?

Private entities in the first instance should turn to the competent national authority forwarding them the personal data which – by their opinion – should be subject to transatlantic transfer, and leave it to the authority to decide and transfer the data accordingly. We fully share and support the opinion of the EDPS, that due to "the uncertainty about the applicable data protection framework" the agreement in any event should not "include the transfer of personal data between private and public parties under the present state of EU law".

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)?

Based on reciprocity data exchanged between EU and US law enforcement authorities can be processed/analyzed by applying the same method agreed and developed jointly by the parties concerned.

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?

The right of access is one of the basic principles to be respected in the agreement. Based on transparency individuals shall have the information about the policy the data controller follows when collecting and processing personal data. Considering this or any other information coming to their knowledge (e.g. directly addressed to them by the data controller) they can make the decision to exercise their right of access and then possibly seek the rectification or erasure their personal data. In certain, well defined cases the data controller may deny rectification or erasure, but the definition must be clear, well established and lawful, and the data subject is to be informed accordingly.

- 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?

Oversight through an independent – e.g. data protection – authority is indispensable anyway. Consequently if the data subject is deprived of the possibility to directly access his personal data, he should at least have the option to turn to the competent authority to exercise the access on and in his behalf.

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?

Yes to both of the questions above. Since the EDPS is an independent authority and has the duties and the powers determined by Regulation (EC) No 45/2001[3], he is undoubtedly the right single point to be provided for in the agreement.

- Should the modalities for transparency and assistance to data subjects by US and EU data protection supervisory authorities be spelled out in the agreement?

Transparency – though it might be limited to ensure the purpose of law enforcement is reached – is one of the basic principles to be respected and reflected in the agreement. Without transparency the person concerned shall not be able to exercise of his rights, especially access to his personal data. Transparency is also a basic prerequisite of the accountability of data controllers.

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?

Certainly yes. Question is which court has the competence. It depends on the territory of origin of the data transferred. Three cases can be differentiated:

If data subjects believe that by gathering and transferring their personal data the competent authority of the country has not respected their data protection rights, they should access to the courts of that country in the first instance.

On the other hand if their data were originally gathered and transmitted unlawfully by an EU organizations, they can turn directly to the European courts.

Thirdly, if the personal data were originally gathered and controlled by an agency in the US, data subjects must have the same right to turn to a US court. Which one and on what legal basis is an open issue, to be properly regulated in the agreement.

- Should laws which discriminate in respect of access to the courts on grounds of nationality or residence be amended?

---

[3] Regulation (EC) No 45/2001 of the European parliament and of the Council of 18 December2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data,

The US Privacy Act of 1974[4] defines "individual" as a citizen of the United States or an alien lawfully admitted for permanent residence, and the right of access to courts is confined to individuals so defined, while the EU DP Directive grants "the right of every person to a judicial remedy". Nevertheless the Directive shall not apply "in any case to processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law".

Although the relevant treaties (ETS no 108 and 181of CoE), the European Convention for the protection of human rights and fundamental freedoms and the Charter of Fundamental Rights of the European Union *strictu sensu* shall apply, and the judicial remedy is provided for in the DP Directive, the new legal instrument based under the Art 16. of the TFEU has to be covered the right of access to court in respect of all kind of activities being under the scope of this legislation without any discrimination.

Consequently both EU and US should ensure in their laws the right of access to court against the unlawful data processing for any data subject without any discrimination.

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.

Since fundamental rights are at issue, both EU and US authorities encounter very serious problems to solve. For us, DP experts of the street it is almost impossible to read through the stunning quantity of documents publicly available. Even then we tried to answer the questions which certainly reflect our up to date knowledge.

Finally, we should fully support the opinion of the EDPS, and strongly hope, the competent bodies shall take it also into consideration.

Budapest, 8 March 2010.

In the name of the association

Dr. Zoltán Alexin, PhD.
senior lecturer
University of Szeged,
H-6720
Árpád tér 2.
Szeged, Hungary
e-mail: alexin@inf.u-szeged.hu
web: http://www.inf.u-szeged.hu/~alexin
Member of the Scientific Advisory Committee
of the
European Privacy Institute

Dr. Pál Könyves Tóth
researcher
Pázmány Péter Catholic University
H-1088
Szentkirályi u. 28-30.
Budapest, Hungary
e-mail: kotopa@jak.ppke.hu

[4] 5 U.S.C. § 552a As Amended