

## **ESBG response to the EC Consultation on the future EU- US international agreement on personal data protection and information sharing for law enforcement purposes**

ESBG (European Savings Banks Group)  
Rue Marie-Thérèse, 11 - B-1000 Brussels  
ESBG Register ID 8765978796-80

**12 March 2010**

## **A. Executive summary**

ESBG is pleased to be given the opportunity to respond to this Consultation. Protection of personal data is a fundamental right of citizens, who expect Member States to take all necessary measures for that right to be upheld. Responding to the security challenges of the 21<sup>st</sup> century – a key mission for governments – should not generate any perception that personal data protection rights can be compromised. Furthermore an effective prevention of terrorist actions calls for cooperation with governments also outside the European Union. A key word in this respect is “cooperation”, where parties to an agreement both within and outside the European Union enjoy the same rights and obligations, and consent that reciprocity is an essential dimension in any cooperation.

This Consultation takes place of course against the background of the history of the “SWIFT” agreement. It is clear that the current situation – a vacuum after the rejection of the draft Interim Agreement by the European Parliament – is much unsatisfactory, also because it may prompt one party to seek and conclude a number of bilateral agreements which may turn out to be the detriment of citizens in the Member States concerned. Therefore a new international agreement must be negotiated as a matter of priority, along the principles laid down in this Position Paper.

ESBG acknowledges that such new international agreement “on personal data protection and information sharing for law enforcement purposes” concerns also other sectors than the banking industry. It therefore recommends that the negotiation aims at the conclusion of a master agreement encompassing all necessary sectors of activity, and that specific areas – such as payments and securities – be addressed via covenants to the master agreement. Work on such covenants could be initiated in parallel to the negotiation of the master agreement.

## **B. Response to the Consultation**

### **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 ?*

This agreement should establish principles and standards for personal data protection applicable to cooperation between countries in the context of law enforcement, and also more specifically principles and standards applicable to processing and transfer of personal data. This agreement should be legally binding. Whilst it is essential that this agreement be the new foundation for trans-Atlantic cooperation between the EU and US, any cooperation between the EU and a third country should as far as possible be based on exactly the same principles and standards.

It can be expected however that such principles and standards will have to be specified by type of data concerned (e.g. financial information vs air passenger information). Therefore such international agreement on data protection and information sharing for law enforcement purposes should be architected as a master agreement, with a number of specific covenants by type of data concerned when indispensable.

## **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) ?*

Regrettably the key concern from a citizen security perspective nowadays is the prevention of terrorist actions. It is therefore recommended that the scope of any such agreement remains narrow, in order to ensure that it contributes materially to attaining the objective of prevention of terrorist actions, and that it can be assessed and reviewed when necessary against this specific objective.

It is furthermore recommended that, to the greatest extent possible, and within the spirit and framework of a co-operation, it is not raw data that is exchanged between authorities, but the output of data analysis by authorities of the party which is requested to contribute information.

Of course the concept of “personal data” will have to be defined very precisely in the agreement under discussion.

- *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) ?*

For the purpose of the agreement to be negotiated “law enforcement” should mean the prevention of terrorist actions, and when necessary the investigation and prosecution of terrorist actions committed.

- *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 ?*

The principles and standards which will be formulated for the purpose of this agreement could be used as benchmark for the formulation when necessary of agreements to support cooperation in other areas. However such other agreements should be negotiated on a case by case basis, in order notably to prevent e.g. a blanket transfer of actual policy making from one party to another.

Furthermore these same principles and standards should be used for negotiating agreements with other countries than the US. Actually the objective should be that the master agreement which will be entered into with the US serves as sample for agreements with other countries – provided the principles formulated herein as respected.

### **2.2. Personal scope**

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

The agreement should establish the principle that if information is to be transferred it must be transferred by government authority to government authority. It will be the responsibility of (a) government authority(ies) in respectively the European Union and the US to set up the required procedures and agreements with the entities (including corporates) that may be required to provide 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 ?*

In exceptional circumstances – e.g. when time is absolutely of the essence, e.g. in the case of air travel – personal data could be transferred by a private entity in one country to a law enforcement authority in another country. Such transfer by a private entity should however be by express delegation of the responsibilities and also rights which will have been granted to the relevant government authority(ies) designated in the agreement under discussion (all government authorities which may provide and/ or receive information must be clearly identified).

It is understood that legislation in some Member States prohibits private entities to provide data to anybody else than e.g. a judge. It is recommended that an exhaustive inventory of such constraints be completed by the Commission's services, so that the agreement under discussion builds on the principle proposed above, yet is aligned with existing legislation.

### **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) ?*

As highlighted earlier in this Position Paper, the notion of “cooperation” should be the essential policy driver for the agreement under discussion. Hence, reciprocity - i.e. one party being able to request the same type/ categories of information, and the same level of assistance, than it commits to provide and grant under the agreement – is an essential element of the agreement under discussion. Any other “one way only” commitment should not be acceptable for Europe.

### **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 ?*

It is understood that “accountability” is meant here in an Anglo-Saxon way. The relevant government authorities will be responsible for evidencing that they conform to the principles of the agreement, and that they process, analyse and transfer data in accordance with data protection principles.

Of course continued adherence to the agreement should be the object of a formal, regular review mechanism – which ideally should be performed by an independent committee with representatives from both parties to the agreement.

#### **4.2. Individual access**

- *Should the agreement spell out the conditions for the right to access one's own personal data ?*

The fundamental right of any individual to access his/ her personal data must be recognized by the agreement. Furthermore the agreement must establish the principle that such access to personal data may not become more onerous to any individual because of the existence of the agreement. In essence, any individual must be able to

access personal collected during the execution of this agreement in the same way he/ she can access other personal data, i.e. in his/her country of residence.

- *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 ?*

Whilst direct access may not be possible in every situation, the conditions for indirect access must be clearly defined in the agreement. Again these conditions must not render access to personal data more onerous for any individual. The relevant government authority(ies), or an independent authority, in the country of residence of the individual concerned, must be responsible for providing such access.

#### **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 ?*

From the perspective of any individual the first and main point of contact must be relevant authorities in his/ her country of residence – as already enunciated above. An individual should be enabled to lodge any concern or complaint with such authority(ies). Of course he/she would not be prevented to lodge a concern or complaint directly with a US authority, if so he/she wishes.

- *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 ?*

Under the concept of reciprocity the same rights and processes as described above should be available to US citizens for data transferred to the EU.

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

Yes, they should be.

#### **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 ?*

In keeping with the principle enunciated earlier in this Position Paper data subjects who believe they have been wronged as a consequence of this agreement must be able to pursue their claim in their country of residence. The agreement (being legally binding) must establish that the competent jurisdiction for any claim is the jurisdiction of the place of residence of the data subject.

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

The agreement should establish the principle that whenever data has been transferred, the individual from one country will not enjoy a lesser protection than an individual in the country to which the data has been transferred would enjoy. Where necessary

discriminating legislation will have to be amended. At a minimum the European Data Protection Directive should be respected.

**5- Any other comment**

The agreement under discussion should be concluded for an indefinite term, provided a clear review mechanism (as described earlier in this Position Paper) is defined and effectively put in place.



### **About ESBG (European Savings Banks Group)**

ESBG (European Savings Banks Group) is an international banking association that represents one of the largest European retail banking networks, comprising about one third of the retail banking market in Europe, with total assets of €5967 billion (1 January 2008). It represents the interest of its members vis-à-vis the EU Institutions and generates, facilitates and manages high quality cross-border banking projects.

ESBG Members are typically savings and retail banks or associations thereof. They are often organised in decentralised networks and offer their services throughout their region. ESBG Member banks have reinvested responsibly in their region for many decades and are one distinct benchmark for corporate social responsibility activities throughout Europe and the world.



European Savings Banks Group - aisbl  
Rue Marie-Thérèse, 11 B-1000 Brussels  
Tel: +32 2 211 11 11  
Fax : +32 2 211 11 99  
[Info@savings-banks.eu](mailto:Info@savings-banks.eu) [www.esbg.eu](http://www.esbg.eu)

Published by ESBG. March 2010