EUROPEAN COMMISSION

MEMO

Brussels, 27 November 2013

Restoring Trust in EU-US data flows - Frequently Asked Questions

What is the Commission presenting today?

Today the European Commission has set out actions to be taken in order to restore trust in data flows between the EU and the U.S., following deep concerns about revelations of large-scale U.S. intelligence collection programmes, which have had a negative impact on the transatlantic relationship.

The Commission's response today takes the form of:

1. **A strategy paper (a Communication) on transatlantic data flows** setting out the challenges and risks following the revelations of U.S. intelligence collection programmes, as well as the steps that need to be taken to address these concerns;
2. **An analysis of the functioning of 'Safe Harbour'** which regulates data transfers for commercial purposes between the EU and U.S.;
3. **A factual report on the findings of the EU-US Working Group** on Data Protection which was set up in July 2013;
4. A **review** of the existing agreements on **Passenger Name Records (PNR)** see MEMO/13/1054),
5. As well as a **review** of the **Terrorist Finance Tracking Programme (TFTP)** regulating data exchanges in these sectors for law enforcement purposes see MEMO/13/1164).

In order to maintain the continuity of data flows between the EU and U.S., a high level of data protection needs to be ensured. The Commission today calls for action in six areas:

1. A swift adoption of the **EU's data protection reform**
2. Making **Safe Harbour** safe
3. Strengthening data protection safeguards in the **law enforcement** area
4. Using the existing **Mutual Legal Assistance** and Sectoral agreements to obtain data
5. Addressing European concerns in the on-going **U.S. reform** process
6. Promoting **privacy standards internationally**

1. The EU's Data Protection Reform: the EU's response to fear of surveillance

How will the EU data protection reform address fears of surveillance?

The EU data protection reform proposed by the Commission in January 2012 (IP/12/46) provides a key response as regards the protection of personal data. Five components of the proposed reform package are of particular importance.

1. **Territorial scope**: the EU data protection reform will ensure that non-European companies, when offering goods and services to European consumers, respect EU data protection law. The fundamental right to data protection will be respected, independently of the geographical location of a company or of its processing facility.
2. **International transfers**: the proposed Regulation establishes clear conditions under which data can be transferred outside the EU. Transfers can only be allowed where these conditions, which safeguard individuals' rights to a high level of protection, are met. The European Parliament, in its vote of 21 October, has even proposed to strengthen these conditions.
3. **Enforcement:** the proposed rules provide for dissuasive sanctions of up to 2% of a company's annual global turnover (the European Parliament has proposed to increase the maximum fines to 5%) to make sure that companies comply with EU law.
4. **Cloud computing**: the Regulation sets out clear rules on the obligations and liabilities of data processors such as cloud providers, including on security. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility by reference to their status as data processors rather than data controllers.
5. **Law Enforcement:** the data protection package will lead to the establishment of comprehensive rules for the protection of personal data processed in the law enforcement sector.

Next Steps: The proposed data protection Regulation and Directive are currently being discussed by the European Parliament and the Council of Ministers. The European Parliament in a vote on 21 October gave its strong backing to the Commission's proposals so that the Parliament is ready to enter negotiations with the second chamber of the EU legislature, the Council of the European Union. European heads of state and government also underlined the importance of a "timely" adoption of the new data protection legislation at a summit on 24 and 25 October 2013. The Commission would like to conclude the negotiations by spring 2014.

2. Making Safe Harbour safer

What is the Safe Harbour Decision?

The 1995 EU Data Protection Directive sets out rules for transferring personal data from the EU to third countries. Under these rules, the Commission may decide that a non-EU country ensures an "adequate level of protection". These decisions are commonly referred to as "adequacy decisions".

On the basis of the 1995 Data Protection Directive, the European Commission, on 26 July 2000, adopted a Decision (the "Safe Harbour decision") recognising the "Safe Harbour Privacy Principles" and "Frequently Asked Questions", issued by the Department of Commerce of the United States, as providing adequate protection for the purposes of personal data transfers from the EU.

As a result, the Safe Harbour decision allows for the free transfer of personal information for commercial purposes from companies in the EU to companies in the U.S. that have signed up to the Principles. Given the substantial differences in privacy regimes between the EU and the U.S., without the Safe Harbour arrangement such transfers would not be possible.

The functioning of the Safe Harbour arrangement relies on commitments and **self-certification** of the companies which have signed up to it. Companies have to sign up to it by notifying the U.S. Department of Commerce while the U.S. Federal Trade Commission is responsible for the enforcement of Safe Harbour. **Signing up to these arrangements is voluntary, but the rules are binding for those who sign up**. The fundamental principles of such an arrangement are:

- Transparency of adhering companies' privacy policies,
- Incorporation of the Safe Harbour principles in companies' privacy policies, and
- Enforcement, including by public authorities.

A U.S. company that wants to adhere to the Safe Harbour must: (a) identify in its publicly available privacy policy that it adheres to the Principles and actually comply with the Principles, as well as (b) self-certify, meaning it has to declare to the U.S. Department of Commerce that it is in compliance with the Principles. The self-certification must be resubmitted on an annual basis.

The U.S. Department of Commerce and the U.S. Federal Trade Commission are responsible for the enforcement of the Safe Harbour scheme in the U.S.

How many companies are using it?

By late-September 2013, the Safe Harbour had a membership of **3246 companies** (an eight-fold increase from 400 in 2004).

Why is Safe Harbour relevant to surveillance?

Under Safe Harbour, limitations to data protection rules are permitted where necessary on grounds of national security, the question has arisen whether the large-scale collection and processing of personal information under U.S. surveillance programmes is necessary and proportionate to meet the interests of national security. Safe Harbour acts as a conduit for the transfer of the personal data of EU citizens from the EU to the U.S. by companies required to surrender data to U.S. intelligence agencies under the U.S. intelligence collection programmes.

How would a review of Safe Harbour work in practice?

Legally speaking, the European Commission is in charge of reviewing the Safe Harbour Decision. The **Commission may maintain the Decision, suspend it or adapt it** in the light of experience with its implementation. This is in particular foreseen in cases of a systemic failure on the U.S. side to ensure compliance, for example if a body responsible for ensuring compliance with the Safe Harbour Privacy Principles in the United States is not effectively fulfilling its role, or if the level of protection provided by the Safe Harbour Principles is overtaken by the requirements of U.S. legislation.

What is the European Commission proposing today with regards to Safe Harbour?

On the basis of a thorough analysis published today and consultations with companies, the European Commission is **making 13 recommendations to improve the functioning of the Safe Harbour scheme**. The Commission is calling on U.S. authorities to identify remedies by summer 2014. The Commission will then review the functioning of the Safe Harbour scheme based on the implementation of these 13 recommendations.

The 13 Recommendations are:

Transparency

1. Self-certified companies should publicly disclose their privacy policies.
2. Privacy policies of self-certified companies' websites should always include a link to the Department of Commerce Safe Harbour website which lists all the 'current' members of the scheme.
3. Self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services.
4. Clearly flag on the website of the Department of Commerce all companies which are not current members of the scheme.

Redress

5. The privacy policies on companies' websites should include a link to the alternative dispute resolution (ADR) provider.
6. ADR should be readily available and affordable.
7. The Department of Commerce should monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.

Enforcement

8. Following the certification or recertification of companies under Safe Harbour, a certain percentage of these companies should be subject to ex officio investigations of effective compliance of their privacy policies (going beyond control of compliance with formal requirements).
9. Whenever there has been a finding of non-compliance, following a complaint or an investigation, the company should be subject to follow-up specific investigation after 1 year.
10. In case of doubts about a company's compliance or pending complaints, the Department of Commerce should inform the competent EU data protection authority.
11. False claims of Safe Harbour adherence should continue to be investigated

Access by US authorities

12. Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.
13. It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate.

Relatively transparent information in this respect is provided by some European companies in Safe Harbour. For **example Nokia**, which has operations in the U.S. and is a Safe Harbour member provides a following notice in its **privacy policy**: *"We may be obligated by mandatory law to disclose your personal data to certain authorities or other third parties, for example, to law enforcement agencies in the countries where we or third parties acting on our behalf operate."*

What are examples of the way in which Safe Harbour functions?

The Safe Harbour scheme allows for the provision of solutions for transfers of personal data in situations where other tools would not be available or not practical.

Orange France is using the cloud computing services of Amazon U.S. for the purposes of data storage. In order for the personal data of Orange France customers to be transferred outside the EU, Amazon U.S. subscribes to the Safe Harbour Principles, which is an alternative to a specific contractual arrangement between the two companies regarding the treatment of personal data transferred to the U.S.

For a global company, such as **Mastercard**, **based in the U.S.** but with a large number of clients in the EU, in order to channel the very large amount of personal data involved in its operations, it cannot have recourse to Binding Corporate Rules as they apply only to transfers within one corporate group. Transfers based on contracts would not work either because thousands would be needed, with different financial institutions. The Safe Harbour scheme offers the flexibility such a global organisation needs for its operations, while permitting the free flow of data outside of the EU, subject to the respect of the Safe Harbour Principles.

3. Strengthening data protection safeguards in the law enforcement area

What is the negotiation of an EU-U.S. data protection 'umbrella agreement' for law enforcement purposes about? What's the objective?

The EU and the U.S. are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation ("umbrella agreement") (IP/10/1661). The EU's objective in these negotiations is to ensure a high level of data protection, in line with the EU data protection acquis, for citizens whose data is transferred across the Atlantic, thereby further strengthening EU-U.S. cooperation in the fights against crime and terrorism.

The conclusion of such an agreement, providing for a high level of protection of personal data, would represent a major contribution to strengthening trust across the Atlantic. Following the EU-U.S. Justice and Home Affairs Ministerial on 18 November, the EU and U.S. committed to "complete the negotiations on the agreement ahead of summer 2014".

What are the demands of the EU in the negotiation?

The high level of protection provided for personal data should be reflected in agreed rules and safeguards on a number of issues:

- Giving EU citizens who are not resident in the U.S. enforceable rights, notably the right to judicial redress. Today, under U.S. law, Europeans who are not resident in the U.S. do not benefit from the safeguards of the 1974 US Privacy Act which limits judicial redress to U.S. citizens and legal permanent residents.

  At the EU-U.S. justice and home affairs ministerial a commitment was made to address this issue: "*We are therefore, as a matter of urgency, committed to advancing rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would act as a basis to facilitate transfers of data in the context of police and judicial cooperation in criminal matters by ensuring a high level of personal data protection for U.S. and EU citizens. We are committed to working to resolve the remaining issues raised by both sides, including judicial redress (a critical issue for the EU). Our aim is to complete the negotiations on the agreement ahead of summer 2014.*"
- Purpose limitation: How and for what purposes the data can be transferred and processed;
- Conditions for and duration of the retention of the data;
- Making sure that derogation based on national security are narrowly defined

An "umbrella agreement" agreed along those lines, should provide the general framework needed to ensure a high level of protection of personal data when transferred to the U.S. for the purpose of preventing or combating crime and terrorism. **The agreement would not provide the legal basis for any specific transfers of personal data** between the EU and the U.S. A specific legal basis for such data transfers would always be required, such as a data transfer agreement or a national law in an EU Member State.

4. Using the existing Mutual Legal Assistance agreement to obtain data

What is the Mutual Legal Assistance agreement (MLA)?

Mutual legal assistance agreements consist of cooperation between different countries for the purpose of gathering and exchanging information, and requesting and providing assistance to obtain evidence located in another country. This also entails requests by law enforcement authorities to assist each other in cross-border criminal investigations or proceedings. Mechanisms have been put in place both in the EU and in the U.S. to provide a framework for these exchanges.

The EU-U.S. Mutual Legal Assistance agreement is in place since 2010. It facilitates and speeds up assistance in criminal matters between the EU and the U.S., including through the exchange of personal information.

If U.S. authorities circumvent the Mutual Legal Assistance agreement and access data directly (through companies) for criminal investigations, they expose companies operating on both sides of the Atlantic to significant legal risks. These companies are likely to find themselves in breach of either EU or U.S. law when confronted with such requests: with U.S. law (such as for example, the Patriot Act) if they do not give access to data and with EU law if they give access to data. A solution would be for the U.S. law enforcement authorities to use formal channels, such as the MLA, when they request access to personal data located in the EU and held by private companies.

Negotiations on the Umbrella Agreement provide an opportunity to agree on commitments that clarify that personal data held by private entities will not be accessed by law enforcement agencies outside of formal channels of co-operation, such as the MLA, except in clearly defined, exceptional and judicially reviewable situations.

What is the U.S. Patriot Act?

The U.S. Patriot Act of 2001 is an Act of Congress that was signed into law by U.S. President George W. Bush on October 26, 2001. It permits the Federal Bureau of Investigation (FBI) to make an application for a court order requiring a business or another entity to produce "tangible things", such as books, records or documents, where the information sought is relevant for an investigation to obtain foreign intelligence information not concerning a U.S. citizens or to protect the country against international terrorism or clandestine intelligence activities. The order is secret and may not be disclosed.

In the course of the EU-U.S. Working Group's meetings, the U.S. confirmed that this Act can serve as the basis for intelligence collection which can include, depending on the programme, telephony metadata (for instance, telephone numbers dialled as well as the date, time and duration of calls) or communications content.

5. Addressing European concerns in the on-going U.S. reform process

How will the U.S. review of U.S. surveillance programmes benefit EU citizens?

U.S. President Obama has announced a review of U.S. national security authorities' activities, including of the applicable legal framework. This on-going process provides an important opportunity to address EU concerns raised following recent revelations about U.S. intelligence collection programmes. The most important changes would be **extending the safeguards available to U.S. citizens and residents to EU citizens not resident in the U.S**., **increased transparency** of intelligence activities, and further **strengthening oversight**.

More transparency is needed on the legal framework of U.S. intelligence collection programmes and its interpretation by U.S. Courts as well as on the quantitative dimension of U.S. intelligence collection programmes. EU citizens would also benefit from such changes.

The oversight of U.S. intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes.

Such changes would restore trust in EU-U.S. data exchanges and in the digital economy.

What about federal U.S. legislation on Privacy?

In March last year, immediately after the Commission's reform proposals were adopted, the White House announced that it would work with Congress to produce a "Consumer Privacy Bill of Rights".

The recent discussions in Congress testify to the growing importance attached to privacy in the U.S as well. An IPSOS poll released in January 2013 says that 45% of U.S. adults feel they have little or no control over their personal data online. In addition, there is also no single U.S. Federal law on data protection. Instead, there is a maze of State laws offering varying degrees of security and certainty. In Florida, not a single law lays down a definition of "personal information". In Arizona there are five. The same goes for rules on security breaches. Some States have them, others do not.

Once a single and coherent set of data protection rules is in place in Europe, we will expect the same from the U.S. This is a necessity to create a stable basis for personal data flows between the EU and the U.S. Inter-operability and a system of self-regulation is not enough. The existence of a set of strong and enforceable data protection rules in both the EU and the U.S. would constitute a solid basis for cross-border data flows.

6. Promoting privacy standards internationally

What can be done at global level?

Issues raised by modern methods of data protection are not limited to data transfer between the EU and the U.S. A high level of protection of personal data should also be guaranteed for any individual. EU rules on collection, processing and transfer of data should be promoted internationally.

The U.S. should accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), as it acceded to the 2001 Convention on Cybercrime.

Will Data Protection standards be part of the on-going negotiations for a Transatlantic Trade and Investment Partnership?

No. Standards of data protection will not be part of the on-going negotiations for a Transatlantic Trade and Investment Partnership. The European Commission makes this very clear in today's Communication.

This has been confirmed by Vice-President Reding and Commissioner de Gucht on several occasions. As Vice-President Reding stated in a recent speech: "*Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable*." (SPEECH/13/867)

7. EU-U.S. Working Group on Data Protection

When was the EU-U.S. Working Group on Data Protection established?

The ad hoc EU-U.S. Working Group on data protection was established in July 2013 to examine issues arising from revelations of a number of U.S. surveillance programmes involving the large-scale collection and processing of personal data. The purpose was to establish the facts around U.S. surveillance programmes and their impact on personal data of EU citizens.

The Council of the European Union also decided to establish a "second track" under which Member States may discuss with the U.S. authorities, in a bilateral format, matters related to national security, and questions related to the alleged surveillance of EU institutions and diplomatic missions.

How many meetings have been held to date?

Four meetings have taken place. A preparatory meeting took place in Washington, D.C. on 8 July 2013. Meetings of the Group took place on 22 and 23 July 2013 in Brussels, on 19 and 20 September 2013 in Washington, D.C., and on 6 November 2013 in Brussels.

Who participates in the Working Group?

On the EU side, the ad hoc Working Group is co-chaired by the Commission and the Presidency of the Council of the European Union. It is composed of representatives of the Presidency, the Commission services (DG Justice and DG Home Affairs), the European External Action Service, the incoming Presidency, the EU Counter-Terrorism Co-ordinator, the Chair of the Article 29 Working Party (in which national data protection authorities meet), as well as ten experts from Member States, selected from the area of data protection and law enforcement/security. On the U.S. side, the group is composed of senior officials from the Department of Justice, the Office of the Director of National Intelligence, the State Department and the Department of Homeland Security.

What have been the main findings of the Working Group?

The main findings of the Working Group have been the following:

- A number of U.S. laws **allow the large-scale collection and processing of personal data** that has been transferred to the U.S. or is processed by U.S. companies, **for foreign intelligence purposes**. The U.S. has confirmed the existence and the main elements of certain aspects of these programmes, under which data collection and processing is done with a basis in U.S. law laying down specific conditions and safeguards.
- **There are differences in the safeguards applicable to EU citizens compared to U.S. citizens whose data is processed**. There is a lower level of safeguards which apply to EU citizens, as well as a lower threshold for the collection of their personal data. In addition, whereas there are procedures regarding the targeting and minimisation of data collection for U.S. citizens, these procedures do not apply to EU citizens, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity. While U.S. citizens benefit from constitutional protections (respectively, First and Fourth Amendments) these do not apply to EU citizens not residing in the U.S.
- **A lack of clarity remains as to the use of some available U.S. legal bases authorising data collection** (such as some 'Executive Order 12333'), the existence of other surveillance programmes, as well as limitations applicable to these programmes.
- Since the orders of the Foreign Intelligence Surveillance Court are secret and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no avenues (judicial or administrative), for either EU or U.S. data subjects to be informed of whether their personal data is being collected or further processed. **There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress.**

- While there is a degree of oversight by the three branches of Government which applies in specific cases, including judicial oversight for activities that imply a capacity to compel information, **there is no judicial approval for how the data collected is queried**: judges are not asked to approve the 'selectors' and criteria employed to examine the data and mine usable pieces of information. There is also no judicial oversight of the collection of foreign intelligence outside the U.S. which is conducted under the sole competence of the Executive Branch.

For more information:

Press release on the EU-U.S. data flows:

IP/13/1166